

527,651

Access to the

14 MAR 2005

10/527651

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2004年4月1日 (01.04.2004)

PCT

(10) 国際公開番号
WO 2004/028072 A1

- (51) 国際特許分類: H04L 9/08, 9/10, 9/32, G09C 1/00
 (21) 国際出願番号: PCT/JP2003/011804
 (22) 国際出願日: 2003年9月17日 (17.09.2003)
 (25) 国際出願の言語: 日本語
 (26) 国際公開の言語: 日本語
 (30) 優先権データ:
 特願2002-273444 2002年9月19日 (19.09.2002) JP
 (71) 出願人(米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
 (72) 発明者; および
 (75) 発明者/出願人(米国についてのみ): 大森 和雄

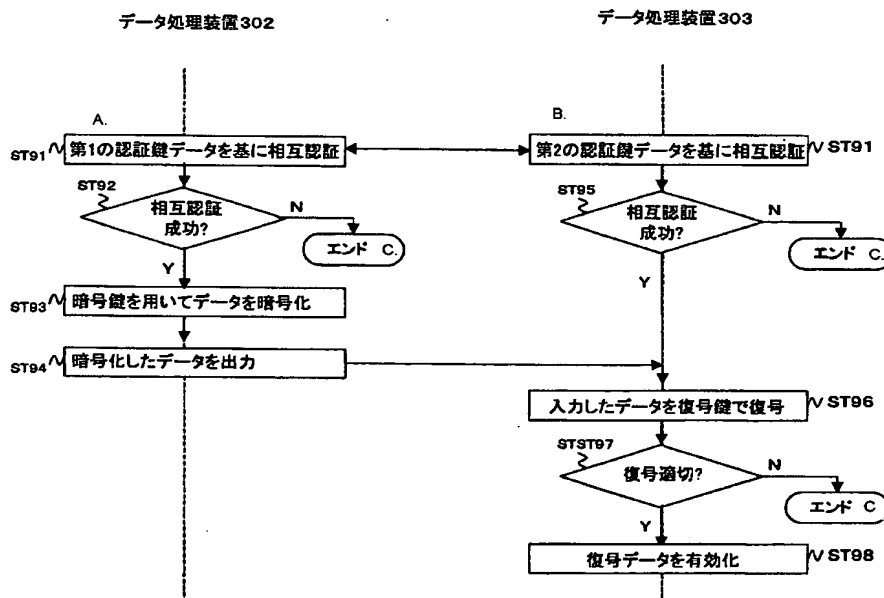
(OMORI, Kazuo) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 本城 哲 (HONJO, Akira) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 末吉 正弘 (SUEYOSHI, Masahiro) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 花木 直文 (HANAKI, Naofumi) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 館野 啓 (TATENO, Kei) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

- (74) 代理人: 佐藤 隆久 (SATO, Takahisa); 〒111-0052 東京都台東区柳橋2丁目4番2号 宮木ビル4階 創造国際特許事務所 Tokyo (JP).

[続葉有]

(54) Title: DATA PROCESSING METHOD, ITS PROGRAM, AND ITS DEVICE

(54) 発明の名称: データ処理方法、そのプログラムおよびその装置



302...DATA PROCESSING DEVICE
 303...DATA PROCESSING DEVICE
 A...PERFORM TWO-WAY AUTHENTICATION USING FIRST AUTHENTICATION KEY DATA SET.
 B...PERFORM TWO-WAY AUTHENTICATION USING SECOND AUTHENTICATION KEY DATA SET.
 ST92...TWO-WAY AUTHENTICATION SUCCESSFUL?
 C...END
 ST93...ENCRYPT DATA USING ENCRYPTION KEY.
 ST94...OUTPUT ENCRYPTED DATA.
 ST96...DECRYPT RECEIVED DATA USING DECRYPTION KEY.
 ST97...DECRYPTION SUCCESSFUL?
 ST98...VALIDATE DECRYPTED DATA.
 ST95...TWO-WAY AUTHENTICATION SUCCESSFUL?

(57) Abstract: Data processing devices (302, 303) authenticates each other using first and second authentication key data sets (ST91). If the two-way authentication is successful, the data processing device (302) encrypts predetermined data using encryption key data and outputs the encrypted data to the data processing device (303) (ST93, ST94). The data processing device (303) decrypts the encrypted data using decryption key data (ST96), judges if the decryption is successful, and validates the data (ST97, ST98).

(57) 要約: データ処理装置 302 と 303 との間で第 1 および第 2 の認証鍵データを用いて相互認証を行う (ST91)。当該相互認証が成功すると、データ処理装置 302 が所定のデータを暗号鍵データを用いて暗号化してデータ処理装置 303 に出力する (ST93, ST94)。データ処理装置 303 は、復号鍵データを用いて上記暗号化データを復号

し (ST96)、それが適切か否かを判断して有効化する (ST97, ST98)。

WO 2004/028072 A1



(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許

(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告書

2 文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

データ処理方法、そのプログラムおよびその装置

5 技術分野

本発明は、認証結果を基に所定の処理を行うデータ処理方法、そのプログラムおよびその装置に関する。

背景技術

- 10 第1のデータ処理装置と第2のデータ処理装置との間で相互認証を行い、お互いの正当性を認証した後に、第1のデータ処理装置から第2のデータ処理装置に暗号化したデータを出力するシステムがある。

このようなシステムでは、上記相互認証と上記データの暗号化とで同じ鍵データを用いている。

- 15 しかしながら、上述した従来のシステムのように、上記相互認証と上記データの暗号化とで同じ鍵データを用いると、相互認証の鍵データが第三者によって不正に取得された場合に、伝送される暗号化データも当該鍵データを用いて不正に解読されてしまうという問題がある。

20 発明の開示

本発明はかかる事情に鑑みてなされたものであり、認証の鍵データが不正に第三者によって取得された場合でも、認証に続いて提供された暗号化データがその第三者によって解読されないようにすることを可能にするデータ処理方法、そのプログラムおよびその装置を提供することを目的とする。

- 25 上述した目的を達成するために、第1の発明のデータ処理方法は、第1のデータ処理装置が第1の認証鍵データおよび暗号鍵データを保持し、第2のデータ処

理装置が前記第 1 の認証鍵データに対応した第 2 の認証鍵データと前記暗号鍵データに対応した復号鍵データとを保持する場合に、前記第 1 のデータ処理装置と前記第 2 のデータ処理装置とが行うデータ処理方法であって、前記第 1 のデータ処理装置が前記第 1 の認証鍵データを用い、前記第 2 のデータ処理装置が前記第 2 の認証鍵データを用いて、前記第 1 のデータ処理装置と前記第 2 のデータ処理装置との間で認証を行う第 1 の工程と、前記第 2 のデータ処理装置が、前記第 1 の工程の前記認証により前記第 1 のデータ処理装置の正当性を認めた場合に、前記第 1 のデータ処理装置が前記暗号鍵データを用いて暗号化を行って前記第 2 のデータ処理装置に提供した暗号化データを、前記復号鍵データを用いて復号する第 2 の工程と、前記第 2 のデータ処理装置が、前記第 2 の工程の前記復号によって得た復号データが適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる第 3 の工程とを有する。

第 1 の発明のデータ処理方法の作用は以下になる。

第 1 の工程において、第 1 のデータ処理装置が第 1 の認証鍵データを用い、第 2 のデータ処理装置が第 2 の認証鍵データを用いて、前記第 1 のデータ処理装置と前記第 2 のデータ処理装置との間で認証を行う。

そして、第 2 の工程において、前記第 2 のデータ処理装置が、前記第 1 の工程の前記認証により前記第 1 のデータ処理装置の正当性を認めた場合に、前記第 1 のデータ処理装置が前記暗号鍵データを用いて暗号化を行って前記第 2 のデータ処理装置に提供した暗号化データを、前記復号鍵データを用いて復号する。

そして、第 3 の工程において、前記第 2 のデータ処理装置が、前記第 2 の工程の前記復号によって得た復号データが適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる。

第 1 の発明のデータ処理方法は、好ましくは、前記第 1 の工程において、前記第 1 のデータ処理装置および前記第 2 のデータ処理装置が、第 1 の暗号化アルゴリズム並びに前記第 1 の暗号化アルゴリズムに対応した第 1 の復号アルゴリズム

を基に、所定のデータの暗号化および復号を行って前記認証を行い、前記第 2 の工程において、前記第 2 のデータ処理装置が、第 2 の暗号化アルゴリズムを基に暗号化された前記暗号化データを、前記第 2 の暗号化アルゴリズムに対応した第 2 の復号アルゴリズムを基に前記復号する。

- 5 また、第 1 の発明のデータ処理方法は、好ましくは、前記第 1 の認証鍵データが所定の鍵データを用いて所定の生成方法で生成されている場合に、前記第 1 の工程は、前記第 1 のデータ処理装置が、前記第 1 の認証鍵データの生成に用いられた鍵データを指定する鍵指定データを前記第 2 のデータ処理装置に提供する第 4 の工程と、前記第 2 のデータ処理装置が、前記第 4 の工程で受けた前記鍵指定
- 10 データが指定する前記鍵データを用いて前記所定の生成手法で前記第 2 の認証鍵データを生成する第 5 の工程と、前記第 1 のデータ処理装置が前記第 1 の認証鍵データを用い、前記第 2 のデータ処理装置が前記第 5 の工程で生成した前記第 2 の認証鍵データを用いて、前記認証を行う第 6 の工程と、前記第 2 のデータ処理装置が、前記第 6 の工程の前記認証により、前記第 1 の認証鍵データと前記第 2
- 15 の認証鍵データとが同じであると判断すると、前記第 1 のデータ処理装置の正当性を認める第 7 の工程とを有する。

- 第 2 の発明のデータ処理システムは、第 1 の認証鍵データおよび暗号鍵データを保持する第 1 のデータ処理装置と、前記第 1 の認証鍵データに対応した第 2 の認証鍵データと前記暗号鍵データに対応した復号鍵データとを保持する第 2 の
- 20 データ処理装置とを有し、前記第 1 のデータ処理装置が、前記第 1 の認証鍵データを用い、前記第 2 のデータ処理装置が前記第 2 の認証鍵データを用いて、前記第 1 のデータ処理装置と前記第 2 のデータ処理装置との間で認証を行い、前記第 2 のデータ処理装置が、前記認証により前記第 1 のデータ処理装置の正当性を認めた場合に、前記第 1 のデータ処理装置が前記暗号鍵データを用いて暗号化を行っ
- 25 て前記第 2 のデータ処理装置に提供した暗号化データを、前記復号鍵データを用いて復号し、前記第 2 のデータ処理装置が、前記復号によって得た復号データが

適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる。

第2の発明のデータ処理システムの作用は以下のようになる。

第1のデータ処理装置が、第1の認証鍵データを用い、第2のデータ処理装置
5 が前記第2の認証鍵データを用いて、第1のデータ処理装置と前記第2のデータ
処理装置との間で認証を行う。

そして、前記第2のデータ処理装置が、前記認証により前記第1のデータ処理
装置の正当性を認めた場合に、前記第1のデータ処理装置が前記暗号鍵データを用
いて暗号化を行って前記第2のデータ処理装置に提供した暗号化データを、前
10 記復号鍵データを用いて復号する。

そして、前記第2のデータ処理装置が、前記復号によって得た復号データが適
切に復号されたものであると判断した場合に、前記復号データを有効なものとし
て用いる。

第3の発明のデータ処理方法は、認証鍵データおよび暗号鍵データを保持する
15 データ処理装置が行うデータ処理方法であって、前記認証鍵データを用いて、認
証先と認証を行う第1の工程と、前記第1の工程の前記認証の後に、前記暗号鍵
データを用いて所定のデータを暗号化する第2の工程と、前記第2の工程の前記
暗号化により得られたデータを前記認証先に出力する第3の工程とを有する。

第4の発明のデータ処理装置は、所定のデータを暗号化して認証先に出力する
20 データ処理装置であって、認証鍵データおよび暗号鍵データを記憶する記憶手段
と、前記認証鍵データを用いて、認証先と認証を行う認証手段と、前記認証手段
の前記認証の後に、前記暗号鍵データを用いて所定のデータを暗号化する暗号化
手段と、前記暗号化手段の前記暗号化により得られたデータを前記認証先に出力
する出力手段とを有する。

25 第5の発明のプログラムは、認証鍵データおよび暗号鍵データを保持するデー
タ処理装置が実行するプログラムであって、前記認証鍵データを用いて、認証先

と認証を行う第 1 の手順と、前記第 1 の手順の前記認証の後に、前記暗号鍵データを用いて所定のデータを暗号化する第 2 の手順と、前記第 2 の手順の前記暗号化により得られたデータを前記認証先に出力する第 3 の手順とを有する。

第 6 の発明のデータ処理方法は、認証鍵データおよび復号鍵データを保持するデータ処理装置が行うデータ処理方法であって、前記認証鍵データを用いて、被認証手段と認証を行う第 1 の工程と、前記復号鍵データを用いて、前記被認証手段から受けたデータを復号する第 2 の工程と、前記第 1 の工程の前記認証により前記被認証手段の正当性を認めると、前記第 2 の工程の前記復号により得られたデータを有効なものとして用いる第 3 の工程とを有する。

第 7 の発明のデータ処理装置は、認証鍵データおよび復号鍵データを保持するデータ処理装置であって、前記認証鍵データを用いて、被認証手段と認証を行う認証手段と、前記被認証手段からデータを入力する入力手段と、前記復号鍵データを用いて、前記入力手段を介して前記被認証手段から入力した前記データを復号する復号手段と、前記認証手段の前記認証により前記被認証手段の正当性を認めると、前記復号手段の前記復号により得られたデータを有効なものとして用いる制御手段とを有する。

第 8 の発明のプログラムは、認証鍵データおよび復号鍵データを保持するデータ処理装置が実行するプログラムであって、前記認証鍵データを用いて、被認証手段と認証を行う第 1 の手順と、前記復号鍵データを用いて、前記被認証手段から受けたデータを復号する第 2 の手順と、前記第 1 の手順の前記認証により前記被認証手段の正当性を認めると、前記第 2 の手順の前記復号により得られたデータを有効なものとして用いる第 3 の手順とを有する。

図面の簡単な説明

図 1 は、本発明の第 1 実施形態に係わるデータ処理システムの構成図である。

図 2 は、図 1 に示す出力側のデータ処理装置の構成図である。

図3は、図1に示す入力側のデータ処理装置の構成図である。

図4は、図1に示すデータ処理システムの動作例を説明するためのフローチャートである。

図5は、本発明の第2実施形態の通信システムの全体構成図である。

5 図6は、図5に示す管理装置の機能ブロック図である。

図7は、図6に示す管理装置が行う処理手順の概要を説明するためのフローチャートである。

図8は、図6に示すAP編集ツールおよび管理ツールに係わる処理において用いられるカードを説明するための図である。

10 図9は、図5に示すICカードの機能ブロック図である。

図10は、図9に示すメモリに記憶されたデータを説明するための図である。

図11は、図5に示すSAMモジュールのソフトウェア構成を説明するための図である。

15 図12は、図5に示すSAMモジュールのハードウェア構成、並びに外部メモリ7の記憶領域を説明するための図である。

図13は、図12に示すAP記憶領域を説明するための図である。

図14は、アプリケーションエレメントデータを説明するための図である。

図15は、アプリケーションエレメントデータAPEのタイプを説明するための図である。

20 図16は、オーナーカードおよびユーザカードの作成手順を説明するためのフローチャートである。

図17は、相互認証鍵データを説明するための図である。

図18は、相互認証コードを説明するための図である。

25 図19Aおよび図19Bは、相互認証鍵データとサービスとの関係を説明するための図である。

図20は、縮退鍵データの生成方法を説明するための図である。

図 2 1 は、縮退鍵データのその他の生成方法を説明するための図である。

図 2 2 は、縮退鍵データの暗号化の階層を説明するための図である。

図 2 3 は、縮退鍵データの特性の一例を説明するための図である。

図 2 4 は、相互認証鍵データの使用形態の一例を説明するための図である。

5 図 2 5 は、図 5 に示す管理装置の S A M 管理機能部と S A M ユニットとの間の相互認証について説明するためのフローチャートである。

図 2 6 は、図 5 に示す管理装置の S A M 管理機能部と S A M ユニットとの間の相互認証について説明するための図 2 5 の続きのフローチャートである。

図 2 7 は、S A M ユニットの処理を説明するためのフローチャートである。

10

発明を実施するための最良の形態

これより図面を参照して本発明の好適実施例について説明していく。

第 1 実施形態

図 1 は、本実施形態に係わるデータ処理システムの構成図である。

15 図 1 に示すように、データ処理システム 3 0 1 は、例えば、データ処理装置 3 0 2 および 3 0 3 を有する。

ここで、データ処理装置 3 0 2 が、第 1 および第 2 の発明の第 1 のデータ処理装置、並びに第 4 の発明のデータ処理装置に対応している。

20 また、データ処理装置 3 0 3 が、第 1 および第 2 の発明の第 2 のデータ処理装置、並びに第 7 の発明のデータ処理装置に対応している。

図 2 は、データ処理装置 3 0 2 の構成図である。

図 2 に示すように、データ処理装置 3 0 2 は、例えば、メモリ 3 1 0、認証部 3 1 1、暗号化部 3 1 2、インタフェース 3 1 3 および CPU 3 1 4 を有し、これらがバス 3 0 9 を介して接続されている。

25 ここで、メモリ 3 1 0 が第 4 の発明の記憶手段に対応し、認証部 3 1 1 が第 4 の発明の認証手段に対応し、暗号化部 3 1 2 が第 4 の発明の暗号化手段に対応し、

インタフェース 313 が第 4 の発明の出力手段に対応している。

メモリ 310 は、第 1 の認証鍵データ 321、暗号鍵データ 322 およびプログラム 323 を記憶している。

ここで、第 1 の認証鍵データ 321 が本発明の第 1 の認証鍵データに対応し、
5 暗号鍵データ 322 が本発明の暗号化データに対応し、プログラム 323 が第 5 の発明のプログラムに対応している。

認証部 311 は、第 1 の認証鍵データ 321 を用いて、データ処理装置 303 と相互認証を行う。

暗号化部 312 は、暗号鍵データ 322 を用いて、所定のデータを暗号化する。

10 インタフェース 313 は、上記暗号化したデータをデータ処理装置 303 に出力する。

CPU 314 は、プログラム 323 を実行して、後述するように、データ処理装置 302 の各構成要素を統括的に処理を行う。

図 3 は、データ処理装置 303 の構成図である。

15 図 3 に示すように、データ処理装置 303 は、例えば、メモリ 330、認証部 331、復号部 332、インタフェース 333 および CPU 334 を有し、これらがバス 339 を介して接続されている。

ここで、メモリ 330 が第 7 の発明の記憶手段に対応し、認証部 331 が第 7 の発明の認証手段に対応し、暗号化部 332 が第 7 の発明の復号手段に対応し、
20 インタフェース 333 が第 7 の発明の入力手段に対応している。

メモリ 330 は、第 2 の認証鍵データ 341、復号鍵データ 342 およびプログラム 343 を記憶している。

ここで、第 2 の認証鍵データ 341 が本発明の第 2 の認証鍵データに対応し、復号鍵データ 342 が本発明の復号データに対応し、プログラム 343 が第 7 の
25 発明のプログラムに対応している。

認証部 331 は、第 2 の認証鍵データ 341 を用いて、データ処理装置 302

と相互認証を行う。

復号部 332 は、復号鍵データ 342 を用いて、インタフェース 333 を介してデータ処理装置 302 から入力したデータを復号する。

5 インタフェース 333 は、データ処理装置 302 から上記暗号化されたデータを入力する。

CPU 334 は、プログラム 343 を実行して、後述するように、データ処理装置 303 の各構成要素を統括的に制御して処理を行う。

以下、図 1 に示すデータ処理システム 301 の動作例を説明する。

10 以下に示す処理は、CPU 314 によるプログラム 323 の実行、並びに CPU 334 によるプログラム 343 の実行に応じて行われる。

・ 図 4 は、当該動作例を説明するためのフローチャートである。

ステップ ST91 :

15 データ処理装置 302 の認証部 311 が第 1 の認証鍵データ 321 を用い、データ処理装置 303 の認証部 331 が第 2 の認証鍵データ 341 を用いて、相互認証を行う。

このとき、認証部 311 および 331 は、それぞれ第 1 の認証鍵データ 321 および 341 を用いて、第 1 の暗号アルゴリズム並びに当該第 1 の暗号アルゴリズムに対応する第 1 の復号アルゴリズムを基に所定のデータの暗号化および復号を行って上記認証を行う。

20 当該相互認証には、第 2 実施形態で後述する相互認証の方法が用いられる。

ステップ ST92 :

データ処理装置 302 の CPU 314 が、ステップ ST91 の相互認証によりデータ処理装置 303 との間でお互いの正当性が認められたと判断した場合にステップ ST93 の処理に進む、そうでない場合には処理を終了する。

25 ステップ ST93 :

データ処理装置 302 の暗号化部 312 が、暗号鍵データ 322 を用いて、第

2の暗号アルゴリズムで所定のデータを暗号化する。

ステップST94：

データ処理装置302のインタフェース313が、ステップST93で暗号化したデータをデータ処理装置303に出力する。

5 ステップST95：

データ処理装置303のCPU334が、ステップST91の相互認証によりデータ処理装置302との間でお互いの正当性が認められたと判断した場合にステップST96の処理に進む、そうでない場合には処理を終了する。

ステップST96：

10 データ処理装置303の復号部332が、復号鍵データ342を用いて、ステップST94でインタフェース333を介してデータ処理装置302から入力した暗号化されたデータを、上記第2の暗号アルゴリズムに対応した第2の復号アルゴリズムで復号する。

ステップST97：

15 データ処理装置303のCPU334が、ステップST96の復号によって得られた復号データが、適切に復号されたものであるか否かを判断し、適切に復号されたものであると判断した場合にはステップST98の処理に進み、そうでない場合には当該復号データを破棄（無効化）する。

ステップST98：

20 データ処理装置303のCPU334が、ステップST97で得られた復号データを有効なものとして用いて処理を行う。

以上説明したように、データ処理システム301によれば、相互認証と暗号化データの生成とを異なる鍵データを用いて行うため、相互認証により用いた第1および第2の認証鍵データが第三者によって不正に取得された場合でも、暗号化

25 データは暗号鍵データを用いて暗号化されているため、当該第三者は当該暗号化データを解読できない。そのため、データ処理システム301によれば、暗号化

データを適切に保護できる。

また、データ処理システム 301 によれば、相互認証と暗号化データの生成とで異なる暗号・復号アルゴリズムを用いているため、相互認証で用いた第 1 の暗号・復号アルゴリズムが第三者に漏れた場合でも、暗号化データは第 2 の暗号アルゴリズムで暗号化されているため、当該第三者は解読できない。

第 2 実施形態

図 5 は、本実施形態の通信システム 1 の全体構成図である。

図 5 に示すように、通信システム 1 は、店舗などに設置されたサーバ装置 2、IC カード 3、カードリーダー・ライター 4、パーソナルコンピュータ 5、ASP (Application Service Provider) サーバ装置 19、SAM (Secure Application Module) ユニット 9a, 9b, ..., 管理装置 20、IC モジュール 42 が内蔵された携帯通信装置 41 を用いて、インターネット 10 を介して通信を行って IC カード 3 あるいは携帯通信装置 41 を用いた決済処理などの手続き処理を行う。

通信システム 1 では、管理装置 20 および SAM ユニット 9a, 9b が本発明に対応した実施の形態に係わる処理を行う。

すなわち、管理装置 20 は、管理者等によって許可された所定の処理を SAM ユニット 9a, 9b に行わせるために用いる IC を内蔵したカード (例えば、後述するオーナーカードおよびユーザカード) を発行する処理を行う。これにより、相互認証に用いられる認証鍵データが被認証手段に対して提供される。

また、管理装置 20 は、上記発行されたカードを管理者やユーザが用いて、SAM ユニット 9a, 9b との間で上記認証鍵データを基に相互認証を行う。

そして、当該相互認証によって互いの正当性が認められると、暗号化鍵データを用いて暗号化された所定の暗号化データが管理装置 20 から SAM ユニット 9a, 9b に出力され、SAM ユニット 9a, 9b が復号鍵データを用いて、当該暗号化データを復号する。

この場合に、管理装置 20 が本発明の第 1 のデータ処理装置および被認証手段

となり、SAMユニット9a, 9bが本発明の第2のデータ処理装置、認証先および認証手段となる。

図6は、管理装置20の機能ブロック図である。

図6に示すように、管理装置20は、例えば、AP編集ツール51、管理ツール52、カードリーダー・ライター53、ディスプレイ54、I/F55および操作部56を有する。

AP編集ツール51および管理ツール52は、データ処理装置でプログラム(第5の発明のプログラム)を実行して実現してもよいし、電子回路(ハードウェア)によって実現してもよい。

10 管理ツール52は、例えば、SAM管理機能部57およびカード管理機能部58を有する。

カードリーダー・ライター53は、以下に示す種々のカードのICとの間で、非接触式あるいは接触式でデータの授受を行う。

15 ディスプレイ54は、カード発行画面やAP管理画面を表示するために用いられる。

I/F55は、SAMユニット9a, 9bとの間で、非接触式あるいは接触式でデータの授受を行う。

操作部56は、AP編集ツール51および管理ツール52に対して、指示やデータを入力ために用いられる。

20 図7は、管理装置20が行う処理手順の概要を説明するためのフローチャートである。

図7において、ステップST2～ステップST4が、図4のステップST91に対応し、ステップST5～ST7が図4のステップST93～ST98に対応している。

25 この場合に、管理装置20がデータ処理装置302に対応し、SAMユニット9a, 9bがデータ処理装置303に対応する。

ステップST1:

管理装置20は、管理者の操作に応じて、カード管理機能部58により、カードリーダ・ライタ53にセットされたデフォルトカード71を用いて、所定のデータが格納されたオーナカード72を作成する。また、オーナカード72を用いてユーザカード73を作成する。

すなわち、管理装置20は、SAMユニット9a, 9b(本発明の認証手段)に係わる処理のうち、オーナカード72およびユーザカード73を用いた被認証手段に許可する処理に関連付けられた相互認証鍵データを用いて、後述するデバイス鍵データを所定の暗号化方法で暗号化して、上記相互認証鍵データを復元困難な縮退鍵データ(本発明の第1の認証鍵データ)を生成する。

そして、管理装置20は、上記生成した縮退鍵データと、当該縮退鍵データの生成に用いた上記相互認証鍵データを指定する鍵指定データとを、オーナカード72およびユーザカード73のICに書き込む。

また、同様に、管理装置20は、トランスポートカード74およびAP暗号化カード75を作成する。

ステップST2:

オーナカード72またはユーザカード73の利用者が、これらのカードを用いて、管理装置20を介して、当該利用者に権限が与えられた処理をSAMユニット9a, 9bに行わせる場合に、上記利用者が管理装置20のカードリーダ・ライタ53に、オーナカード72またはユーザカード73のICに記憶された上記鍵指定データを読み込ませる。

管理装置20のSAM管理機能部57は、当該読み込んだ鍵指定データをSAMユニット9a, 9bに出力する。

ステップST3:

SAMユニット9a, 9bが、上記鍵指定データが指定する相互認証鍵データを用いて、上記デバイス鍵データを上記所定の暗号化方法で暗号化して縮退鍵デ

ータ（本発明の第2の認証鍵データ）を生成する。

ステップST4：

SAM管理機能部57がカード72または73から読み出した縮退鍵データを用い、SAMユニット9a、9bが上記生成した縮退鍵データを用いて、第1の

5 暗号化アルゴリズムおよび第1の復号アルゴリズムを基に相互認証を行う。

ステップST5：

ステップST4の相互認証により互いの正当性が認められると、管理装置20が、暗号鍵データを用いて、第2の暗号化アルゴリズムで所定のデータを暗号化してSAMユニット9a、9bに出力する。

10 ステップST6：

SAMユニット9a、9bが、復号鍵データを用いて、ステップST5で入力した暗号化されたデータを、上記第2の暗号アルゴリズムに対応した第2の復号アルゴリズムで復号する。

ステップST7：

15 SAMユニット9a、9bが、ステップST6の復号データが、適切に復号されたものであるか否かを判断し、適切に復号されたものであると判断した場合には、ステップST6で得られた復号データを有効なものとして用いて、オーナカード72等に許可した上記鍵データに関連付けられた処理を実行する。

一方、SAMユニット9a、9bが、上記復号データが適切に復号されたもの
20 ではないと判断した場合には、当該復号データを破棄（無効化）する。

図8は、図6に示すAP編集ツール51および管理ツール52に係わる処理において用いられるカードを説明するための図である。

図8に示すように、管理装置20の管理ツール52を用いて、SAMユニット9a、9bにアクセスする場合に、オーナカード72およびユーザカード73が
25 用いられる。

また、AP編集ツール51で生成したAPパッケージファイルを管理ツール5

2 に提供する場合に、AP暗号化カード75のICに記憶された暗号化鍵データを用いて、当該APパッケージファイルが暗号化される。

すなわち、図8に示すように、ユーザが、AP編集ツール51を用いて、SAMモジュール8内のアプリケーションプログラムAPを構成するアプリケーション
5 エlementデータAPEを作成する。

そして、AP編集ツール51が、単数または複数のアプリケーションElement
トデータAPEを含むAPパッケージファイルを作成し、これをAP暗号化カード75に格納された暗号鍵データを用いて暗号化して管理ツール52に提供する。

管理ツール52は、上述したように、SAMユニット9a、9bと相互認証を
10 行い、当該相互認証に用いた相互認証鍵データに関連付けて許可されたSAM
ユニット9a、9b内のAP記憶領域に対して、AP編集ツール51から受けたA
Pパッケージファイルを書き込む。

また、トランスポートカード74は、SAMユニット9a、9bが保持する鍵
データなどのセキュリティに係わるデータを取り出して他の機器に転送したり、
15 保存等するために用いられる。

〔ICカード3および携帯通信装置41〕

図9は、ICカード3の機能ブロック図である。

図9に示すように、ICカード3は、メモリ50およびCPU51を備えたI
C(Integrated Circuit)モジュール3aを有する。

20 メモリ50は、図10に示すように、クレジットカード会社などのサービス事
業者15__1が使用する記憶領域55__1、サービス事業者15__2が使用する
記憶領域55__2、並びにサービス事業者15__3が使用する記憶領域55__3
を有する。

また、メモリ50は、記憶領域55__1へのアクセス権限を判断するために用
25 いる鍵データ、記憶領域55__2へのアクセス権限を判断するために用い
れる鍵データ、並びに記憶領域55__3へのアクセス権限を判断するために用い

られる鍵データを記憶している。当該鍵データは、相互認証や、データの暗号化および復号などに用いられる。

また、メモリ50は、ICカード3あるいはICカード3のユーザの識別データを記憶している。

- 5 携帯通信装置41は、携帯電話網およびインターネット10を介してASPサーバ装置19a、19bと通信を行う通信処理部43と、通信処理部43との間でデータ授受可能なICモジュール42とを有し、アンテナからインターネット10を介してSAMユニット9aと通信を行う。

- 10 ICモジュール42は、携帯通信装置41の通信処理部43とデータ授受を行う点を除いて、前述したICカード3のICモジュール3aと同じ機能を有している。

- なお、携帯通信装置41を用いた処理は、ICカード3を用いた処理と同様に行われ、ICモジュール42を用いた処理はICモジュール3aを用いた処理と同様に行われるため、以下の説明では、ICカード3およびICモジュール3a
15 を用いた処理について例示する。

以下、SAMユニット9a、9bについて説明する。

図5に示すように、SAMユニット9a、9bは、外部メモリ7とSAMモジュール8とを有する。

- 20 ここで、SAMモジュール8は、半導体回路として実現してもよいし、筐体内に複数の回路を収容した装置として実現してもよい。

〔SAMモジュール8のソフトウェア構成〕

SAMモジュール8は、図11に示すようなソフトウェア構成を有している。

- 25 図11に示すように、SAMモジュール8は、下層から上層に向けて、ハードウェアHW層、周辺HWに対応したRTOSカーネルなどを含めたドライバ層(OS層)、論理的にまとまった単位の処理を行う下位ハンドラ層、アプリケーション固有のライブラリなどをまとめた上位ハンドラ層およびAP層を順に有している。

ここで、AP層では、図5に示すクレジットカード会社などのサービス事業者15__1, 15__2, 15__3によるICカード3を用いた手続きを規定したアプリケーションプログラムAP__1, AP__2, AP__3が、外部メモリ7から読み出されて動作している。

- 5 AP層では、アプリケーションプログラムAP__1, AP__2, AP__3相互間、並びに上位ハンドラ層との間にファイアウォールFWが設けられている。

〔SAMモジュール8のハードウェア構成〕

図12は、SAMモジュール8のハードウェア構成、並びに外部メモリ7の記憶領域を説明するための図である。

- 10 図12に示すように、SAMモジュール8は、例えば、メモリI/F61、外部I/F62、メモリ63、認証部64およびCPU65を有し、これらがバス60を介して接続されている。

また、SAMモジュール8が、第7の発明のデータ処理装置に対応し、以下に示す各手順を含むプログラムを実行して、その機能を実現してもよい。

- 15 メモリI/F61は、外部メモリ7との間でデータ授受を行う。

外部I/F62は、図5に示すASPサーバ装置19a, 19bおよび管理装置20との間で、データおよびコマンドの授受を行う。

メモリ63は、後述するSAMユニット9a, 9bの相互認証などに用いられる種々の鍵データなどを記憶する。当該鍵データは、外部メモリ7のAP管理用

- 20 記憶領域221に記憶されていてもよい。

認証部64は、後述する相互認証に係わる処理を行う。認証部64は、例えば、所定の鍵データを用いた暗号化および復号などを処理を行う。

CPU65は、SAMモジュール8の処理を統括して制御する。

- 25 CPU65は、後述するように、相互認証で正当な相手であることを確認すると、被認証手段に対して、後述する相互認証鍵データに関連付けられた処理を許可し、これを実行する。

SAMモジュール8による相互認証処理については、後に詳細に説明する。

〔外部メモリ7〕

図12に示すように、外部メモリ7の記憶領域には、サービス事業者15__1のアプリケーションプログラムAP__1が記憶されるAP記憶領域220__1 (サービスAPリソース領域)、サービス事業者15__2のアプリケーションプログラムAP__2が記憶されるAP記憶領域220__2、サービス事業者15__3のアプリケーションプログラムAP__3が記憶されるAP記憶領域220__3、並びにSAMモジュール208の管理者が使用するAP管理用記憶領域221 (システムAPリソース領域および製造者APリソース領域) がある。

10 AP記憶領域220__1に記憶されているアプリケーションプログラムAP__1は、図13に示すように、後述する複数のアプリケーションエレメントデータAPEによって構成されている。AP記憶領域220__1へのアクセスは、ファイアウォールFW__1 (図12に図示) によって制限されている。

15 AP記憶領域220__2に記憶されているアプリケーションプログラムAP__2は、図13に示すように、複数のアプリケーションエレメントデータAPEによって構成されている。AP記憶領域220__2へのアクセスは、ファイアウォールFW__2 (図12に図示) によって制限されている。

20 AP記憶領域220__3に記憶されているアプリケーションプログラムAP__3は、図13に示すように、複数のアプリケーションエレメントデータAPEによって構成されている。AP記憶領域220__3へのアクセスは、ファイアウォールFW__3 (図12に図示) によって制限されている。

本実施形態では、上記アプリケーションエレメントデータAPEは、例えば、SAMユニット9aの外部から外部メモリ7にダウンロードされる最小単位である。各アプリケーションプログラムを構成するアプリケーションエレメントデータAPEの数は、対応するサービス事業者が任意に決定できる。

また、アプリケーションプログラムAP__1, AP__2, AP__3は、例えば、

それぞれ図5に示すパーソナルコンピュータ15__1, 15__2, 15__3を用いて、サービス事業者16__1, 16__2, 16__3によって作成され、SAMモジュール8を介して外部メモリ7にダウンロードされる。

5 なお、AP管理用記憶領域221に記憶されたプログラム、並びにデータも、
上述したアプリケーションエレメントデータAPEを用いて構成されている。

図14は、上述したアプリケーションエレメントデータAPEを説明するための図である。

10 アプリケーションエレメントデータAPEは、図14に示すように、APEの属性（種別）を基に規定された分類を示すAPEタイプによって規定されたインスタンスを用いて構成される。

各インスタンスは、エレメントIDと、エレメントプロパティと、エレメントバージョンとによって規定されている。

15 APEタイプを基に、当該アプリケーションエレメントデータAPEが、図12に示すサービスAP記憶領域220__1, 220__2, 220__3およびAP管理用記憶領域221の何れに格納されるかが規定される。

サービスAP記憶領域220__1は、各サービス事業者がアクセス可能なデータを記憶する。

20 なお、AP管理用記憶領域221は、システムの管理者がアクセス可能なデータを記憶するシステムAP記憶領域（図示せず）と、システムの製造者がアクセス可能なデータを記憶する製造者AP記憶領域（図示せず）とを有する。

また、サービスAP記憶領域220__1, 220__2, 220__3およびAP管理用記憶領域221によって、AP記憶領域が構成される。

25 本実施形態では、上述したサービスAP記憶領域220__1, 220__2, 220__3およびAP管理用記憶領域221の各々にはID（AP記憶領域ID）が割り当てられており、APEタイプ、インスタンス、並びにエレメントバージョンの各々には識別用の番号（APEタイプ番号、インスタンス番号、並びにエ

レメントバージョン番号) が割り当てられている。

図15は、APEタイプの一例を説明するための図である。

図15に示すように、APEタイプには、ICシステム鍵データ、ICエリア
鍵データ、ICサービス鍵データ、IC縮退鍵データ、IC鍵変更パッケージ、
5 IC発行鍵パッケージ、IC拡張発行鍵パッケージ、ICエリア登録鍵パッケージ、
ICエリア削除鍵パッケージ、ICサービス登録鍵パッケージ、ICサービ
ス削除鍵パッケージ、ICメモリ分割鍵パッケージ、ICメモリ分割素鍵パッケ
ージ、障害記録ファイル、相互認証用鍵、パッケージ鍵、ネガリストおよびサー
ビスデータテンポラリファイルがある。

10 各APEタイプには、APEタイプ番号が割り当てられている。

以下、図15に示すAPEタイプのうち一部を説明する。

ICシステム鍵データ、ICエリア鍵データ、ICサービス鍵データおよびI
C縮退鍵データは、ICカード3およびICモジュール42のメモリ50に対し
てのデータの読み書き操作に用いられるカードアクセス鍵データである。

15 相互認証用鍵データ同一SAM内にあるAP間相互認証にも使用される。SA
M相互認証用鍵データとは、対応するアプリケーションエレメントデータAPE
を同一SAM内の他のAPまたは他のSAMからアクセスする際に用いられる鍵
データである。

ICメモリ分割用鍵パッケージは、サービス事業者がICカード3を用いたサ
20 ービスの運用開始前に、外部メモリ7やICカード3のメモリの記憶領域を分割
するために使用するデータである。

ICエリア登録鍵パッケージは、サービス事業者がICカード3を用いたサー
ビスの運用開始前に、ICカード3のメモリの記憶領域にエリア登録を行う場合
に使用するデータである。

25 ICエリア削除用鍵パッケージは、カードアクセス鍵データからSAM内部で
自動生成が可能なパッケージである。

ICサービス登録用鍵パッケージは、サービス事業者がICカード3を用いたサービスの運用開始前に、外部メモリ7のアプリケーションエレメントデータAPEを登録するために用いられる。

ICサービス削除用鍵パッケージは、外部メモリ7に登録されているアプリケーションエレメントデータAPEを削除するために用いられる。

〔オーナーカード72およびユーザカード73の作成〕

図16は、オーナーカード72およびユーザカード73の作成手順を説明するためのフローチャートである。

図16は、図7に示すステップST1を詳細に示すものである。

10 ステップST11：

例えば、管理者が、オーナーカード72を作成する場合には、オーナーカード72の使用者に許可するSAMユニット9a、9bに係わる処理を選択する。

また、管理者等が、ユーザカード73を作成する場合に、ユーザカード73の使用者に許可するSAMユニット9a、9bに係わる処理を選択する。

15 SAMユニット9a、9bに係わる処理には、例えば、SAMユニット9a、9bが提供する機能を実行する処理、またはSAMユニット9a、9bが保持するデータ（例えば、アプリケーションエレメントデータAPE）へのアクセスなどがある。

ステップST12：

20 管理者等が、ステップST11で選択した処理に関連付けられた相互認証鍵データを選択して、管理装置20のカード管理機能部58に入力あるいは指定する。

当該相互認証鍵データについては後に詳細に説明する。

ステップST13：

25 管理装置20のカード管理機能部58が、ステップST12で選択された単数または複数の相互認証鍵データを用いて後述する縮退処理方法を基に縮退鍵データを生成する。

当該縮退処理については後に詳細に説明する。

ステップST14：

管理装置20のカード管理機能部58が、ステップST13で縮退鍵データの生成に用いた、相互認証鍵データを識別する相互認証コードを示す鍵指定データを生成する。

当該鍵指定データは、オーナーカード72またはユーザカード73の使用者が取得した、SAMユニット9a, 9bに係わる処理の実行権限を示すデータとなる。

ステップST15：

管理装置20のカード管理機能部58が、ステップST13で生成した縮退鍵データと、ステップST14で生成した鍵指定データとを、オーナーカード72またはユーザカード73のICに書き込む。

ステップST16：

管理装置20のカード管理機能部58が、ステップST13の縮退鍵データの生成に用いた、相互認証鍵データをSAMユニット9a, 9bに登録する。

以下、上述した図16に示すステップST12で選択する対象となる相互認証鍵データについて説明する。

図17は、図16に示すステップST12で選択する対象となる相互認証鍵データを説明するための図である。

図17に示すように、当該相互認証鍵データには、例えば、デバイス鍵データ、ターミネーション鍵データ、製造設定サービス相互認証鍵データ、機器管理サービス相互認証鍵データ、通信管理サービス相互認証鍵データ、相互認証サービス相互認証鍵データ、AP記憶領域管理サービス相互認証鍵データ、サービスAP記憶領域相互認証鍵データ、システムAP記憶領域相互認証鍵データ、並びに製造者AP記憶領域相互認証鍵データがある。

また、図17および図18に示すように、相互認証鍵データの相互認証コードが、図14を用いて説明したAP記憶領域ID、エレメントタイプ番号、エレメ

ントインスタンス番号およびエレメントバージョン番号から構成される。

以下、上述した図 1 6 に示すステップ S T 1 4 で生成する鍵指定データについて説明する。

5 当該鍵指定データは、上述した複数の相互認証鍵データの相互認証コードを用いて構成される、相互認証コードリストである。

図 1 9 A および図 1 9 B は、鍵指定データの一例を説明するための図である。

10 図 1 6 のステップ S T 1 2 で、例えば、図 1 7 に示すデバイス鍵データ、機器管理サービス相互認証鍵データ、通信管理サービス相互認証鍵データ、A P 記憶領域管理サービス相互認証鍵データ、サービス A P 記憶領域相互認証鍵データ、並びにターミネーション鍵データが選択された場合には、図 1 9 A に示すように、当該選択された全ての相互認証鍵データの相互認証コードを示す鍵指定データが生成される。

15 図 1 6 に示すステップ S T 1 3 において、図 1 9 A に示す相互認証コードの相互認証鍵データを用いて縮退鍵データが生成された場合には、当該縮退鍵データを用いた S A M ユニット 9 a, 9 b との相互認証により、管理装置 2 0 に対して、図 1 9 B に示すように、機器管理サービス、通信管理サービス、I C サービス (I C カード 3 および I C モジュール 4 2 1 に関するサービス)、相互認証サービスおよび A P 記憶領域管理サービスが許可される。

20 このように、本実施形態では、S A M ユニット 9 a, 9 b の機能と、S A M ユニット 9 a, 9 b が保持するデータ (例えば、アプリケーションエレメントデータ A P E) へのアクセスを含む複数の処理にそれぞれ関連付けられた相互認証鍵データを用いて縮退鍵データを生成できる。

25 これにより、単数の縮退鍵データを用いた相互認証により、S A M ユニット 9 a, 9 b が、S A M ユニット 9 a, 9 b の機能と、S A M ユニット 9 a, 9 b が保持するデータへのアクセスとの双方について、それらを被認証手段に対して許可するか否かを一括して判断できる。

そして、SAMユニット9a、9bは、被認証手段が正当であると認証した場合に、当該被認証手段の指示に応じて、上記相互認証鍵データに関連付けられた所定の機能に係わる処理を実行すると共に、SAMユニット9a、9bが保持するデータへの上記被認証手段からのアクセスを許可する。

5 以下、図16に示すステップST13の縮退処理方法について説明する。

図20は、当該縮退処理方法を説明するためのフローチャートである。

ステップST21：

管理装置20のカード管理機能部58が、デバイス鍵データをメッセージとし、
図16に示すステップST12で選択されたデバイス鍵データおよびターミネー
10 ション鍵データ以外の相互認証鍵データのうち最初の一つを暗号鍵として用いて、
デバイス鍵データを暗号化し、中間鍵データを生成する。

ここで、ステップST12で選択されたデバイス鍵データおよびターミネー
ション鍵データ以外の相互認証鍵データが一つの場合には、カード管理機能部58
は、上記中間鍵データを用いて次のステップST22の処理を行う。

15 一方、ステップST12で選択されたデバイス鍵データおよびターミネー
ション鍵データ以外の相互認証鍵データが2以上の場合には、カード管理機能部58
は、上記中間鍵データをメッセージとして、次の相互認証鍵データを暗号鍵とし
て用いて暗号化を行う。

カード管理機能部58は、ステップST12で選択されたデバイス鍵データお
20 よびターミネーション鍵データ以外の全ての相互認証鍵データを暗号鍵として用
いて上記暗号化を行うまで上記処理を繰り返し、終了したらステップST22の
処理に進む。

ステップST22：

カード管理機能部58が、ステップST21で得られた中間鍵データをメッセ
25 ージとして、ターミネーション鍵データを暗号鍵として用いて暗号化を行って縮
退鍵データを生成する。

当該ターミネーション鍵データは、改竄防止鍵データであり、管理者のみが保持している。

これにより、管理者以外の者が、不正に縮退鍵データを改竄することを防止できる。

- 5 以下、上述したターミネーション鍵データとして、管理者（オーナー）のみが所有するオーナーターミネーション鍵データと、上記管理者から権限を与えられたユーザが所有するユーザターミネーション鍵データとを用いて、所定の縮退処理方法で、縮退鍵データを生成する場合を説明する。

図21は、当該縮退処理方法を説明するためのフローチャートである。

- 10 図21において、ステップST31、ST32の処理は、ターミネーション鍵データとして、上記オーナーターミネーション鍵データを用いる点を除いて、図20を用いて説明したステップST21、ST22の処理と同じである。

ステップST32で生成された縮退鍵データは、ユーザターミネーション鍵データを与えられたユーザが、拡張できるという意味で拡張可能な縮退鍵データである。

ステップST33：

- 管理装置20のカード管理機能部58が、オーナーが生成した拡張可能縮退鍵データをメッセージとし、ユーザが選択したユーザターミネーション鍵データ以外の相互認証鍵データのうち最初の一つを暗号鍵として用いて、デバイス鍵データを暗号化し、中間鍵データを生成する。

ここで、上記選択されたユーザターミネーション鍵データ以外の相互認証鍵データが一つの場合には、カード管理機能部58は、上記中間鍵データを用いて次のステップST22の処理を行う。

- 25 一方、上記選択されたユーザターミネーション鍵データ以外の相互認証鍵データが2以上の場合には、カード管理機能部58は、上記中間鍵データをメッセージとして、次の相互認証鍵データを暗号鍵として用いて暗号化を行う。

カード管理機能部 58 は、上記選択されたユーザーミネーション鍵データ以外の全ての相互認証鍵データを暗号鍵として用いて上記暗号化を行うまで上記処理を繰り返し、終了したらステップ S T 3 4 の処理に進む。

ステップ S T 3 4 :

- 5 カード管理機能部 58 が、ステップ S T 3 3 で得られた中間鍵データをメッセージとして、ユーザーミネーション鍵データを暗号鍵として用いて暗号化を行って縮退鍵データを生成する。

当該ユーザーミネーション鍵データは、改竄防止鍵データであり、上記オーナーおよび上記ユーザのみが保持している。

- 10 これにより、上記オーナーおよび上記ユーザ以外の者が、不正に縮退鍵データを改竄することを防止できる。

図 2 1 に示す処理によって生成された縮退鍵データは、図 2 2 に示すような階層で相互認証鍵が暗号化されたものになる。

- 15 また、本実施形態では、単数の相互認証鍵データ（例えば、図 1 7 に示すサービス、システム、製造者 A P 記憶領域相互認証鍵データ）に、複数のアプリケーションエレメントデータ A P E を関連付けてもよい。

これにより、縮退鍵データを用いた認証により、S A M ユニット 9 a , 9 b が、単数の相互認証鍵データに関連付けられたアプリケーションエレメントデータ A P E へのアクセスを許可するか否かを一括して判断できる。

- 20 例えば、図 2 3 では、相互認証鍵データ 5 0 0 に、アプリケーションエレメントデータ A P E のインスタンス a のパーミッション C と、インスタンス b のパーミッション B とが関連付けられている。そのため、相互認証鍵データ 5 0 0 を縮退した縮退鍵データを用いた認証が成功すれば、S A M ユニット 9 a , 9 b がインスタンス a , b の双方へのアクセスを許可する。

- 25 本実施形態では、図 1 7 を用いて説明した相互認証鍵データの全てある一部について、図 2 4 に示すように、オンライン相互認証鍵データ M K 1 とオフライン

相互認証鍵データMK 2とをペアで用いる。

この場合には、相互認証を行う場合にはオンライン鍵データMK 1を用い、相互認証を行った相手とはデータ授受を行う場合には、それに対応するオフライン鍵データMK 2を用いて授受するデータを暗号化する。

- 5 これにより、仮にオンライン鍵データMK 1が不正に他人に取得された場合でも、被認証手段と認証手段とで授受するデータはオフライン鍵データMK 2で暗号化されているため、その情報が不正に漏れることを防止できる。

- すなわち、第1実施形態における第1の認証鍵データ3 2 1がオンライン鍵データMK 1に対応し、第1実施形態における暗号鍵データ3 2 2がオフライン鍵データMK 2に対応している。また、第1実施形態における第2の認証鍵データ3 4 1がオンライン鍵データMK 1に対応し、第1実施形態における復号鍵データ3 4 2がオフライン鍵データMK 2に対応している。
- 10

- 以下、例えば、図7に示すステップST 3などで行われる管理装置20のSAM管理機能部57とSAMユニット9 a、9 bとの間の相互認証について説明する。
- 15

この場合に、管理装置20が被認証手段となり、SAMユニット9 a、9 bが認証手段となる。

図25および図26は、管理装置20のSAM管理機能部57とSAMユニット9 aとの間の相互認証について説明するためのフローチャートである。

- 20 SAMユニット9 bについても、以下に示すSAMユニット9 aの場合と同じである。

ステップST 51：

先ず、管理者またはユーザが、オーナカード72またはユーザカード73を、カードリーダー・ライター53にセットする。

- 25 そして、オーナカード72およびユーザカード73に記憶された縮退鍵データK a（本発明の第1の認証鍵データ）および鍵指定データが、管理装置20のS

AM管理機能部 57 に読み込まれる。

SAM管理機能部 57 が、乱数 R_a を発生する。

ステップ ST 52 :

5 SAM管理機能部 57 が、ステップ ST 51 で読み込んだ縮退鍵データ K_a を用いて、ステップ ST 51 で生成した乱数 R_a を、暗号化アルゴリズム 1 で暗号化してデータ R_a' を生成する。

ステップ ST 53 :

SAM管理機能部 57 が、ステップ ST 51 で読み込んだ鍵指定データと、ステップ ST 52 で生成したデータ R_a' とを SAMユニット 9a に出力する。

10 SAMユニット 9a は、図 12 に示す外部 I/F 62 を介して、当該鍵指定データおよびデータ R_a' を入力して、これをメモリ 63 に格納する。

ステップ ST 54 :

15 SAMユニット 9a の認証部 64 が、メモリ 63 あるいは外部メモリ 7 に記憶された相互認証鍵データのなかから、ステップ ST 53 で入力した鍵指定データが示す相互認証鍵データを特定する。

ステップ ST 55 :

SAMユニット 9a の認証部 64 が、ステップ ST 54 で特定した相互認証鍵データを用いて、図 20 あるいは図 21 を用いて前述した縮退処理を行って縮退鍵データ K_b を生成する。

20 ステップ ST 56 :

SAMユニット 9a の認証部 64 が、ステップ ST 55 で生成した縮退鍵データ K_b を用いて、上記暗号化アルゴリズム 1 に対応した復号アルゴリズム 1 で、ステップ ST 53 で入力したデータ R_a' を復号して乱数 R_a を生成する。

ステップ ST 57 :

25 SAMユニット 9a の認証部 64 が、上記縮退鍵データ K_b を用いて、暗号化アルゴリズム 2 で、ステップ ST 56 で生成した乱数 R_a を暗号化して、データ

R a'' を生成する。

ステップST 5 8 :

SAMユニット9 aの認証部6 4が、乱数R bを生成する。

ステップST 5 9 :

- 5 SAMユニット9 aの認証部6 4が、上記縮退鍵データK bを用いて、ステップST 5 8で生成した乱数R bを、暗号化アルゴリズム2で暗号化してデータR b' を生成する。

ステップST 6 0 :

- 10 SAMユニット9 aの認証部6 4が、ステップST 5 7で生成したデータR a''と、ステップST 5 9で生成したデータR b'とを管理装置2 0に出力する。

ステップST 6 1 :

管理装置2 0のSAM管理機能部5 7が、縮退鍵データK aを用いて、上記暗号化アルゴリズム2に対応した復号アルゴリズム2で、ステップST 6 0で入力したデータR a'' およびR b' を復号してデータR a, R bを生成する。

- 15 ステップST 6 2 :

管理装置2 0のSAM管理機能部5 7が、ステップST 5 1で生成した乱数R aと、ステップST 6 1で生成したデータR aとを比較する。

- そして、SAM管理機能部5 7が、上記比較と結果が同じであることを示す場合に、SAMユニット9 aが保持する上記縮退鍵データK bが、SAM管理機能部5 7が保持する上記縮退鍵データK aと同じであり、SAMユニット9 aが正
20 当な認証手段であると認証する。

ステップST 6 3 :

管理装置2 0のSAM管理機能部5 7が、縮退鍵データK aを用いて、暗号化アルゴリズム1で、ステップST 6 1で生成したデータR bを暗号化して、データR b'' を生成する。

- 25

ステップST 6 4 :

管理装置 20 の SAM 管理機能部 57 が、ステップ ST 63 で生成したデータ R b'' を SAM ユニット 9 a に出力する。

ステップ ST 65 :

5 SAM ユニット 9 a の認証部 64 が、縮退鍵データ K b を用いて、ステップ ST 64 で入力したデータ R b'' を、復号アルゴリズム 1 で復号してデータ R b を生成する。

ステップ ST 66 :

SAM ユニット 9 a の認証部 64 が、ステップ ST 58 で生成した乱数 R b と、ステップ ST 65 で生成したデータ R b とを比較する。

10 そして、認証部 64 が、上記比較と結果が同じであることを示す場合に、SAM ユニット 9 a が保持する上記縮退鍵データ K b が、SAM 管理機能部 57 が保持する上記縮退鍵データ K a と同じであり、SAM 管理機能部 57 が正当な被認証手段であると認証する。

15 上述した図 25 および図 25 を用いて説明した相互認証方法は、例えば、図 4 に示すステップ ST 91 の相互認証で用いてもよい。

この場合には、データ処理装置 302 が上述した管理装置 20 に対応した処理を行い、データ処理装置 303 が上述した SAM ユニット 9 a, 9 b に対応した処理を行う。

20 以下、図 25 および図 26 を用いて説明した相互認証の結果を基に、SAM ユニット 9 a, 9 b が行う処理を説明する。

図 27 は、SAM ユニット 9 a, 9 b の処理を説明するための図である。

ステップ ST 71 :

25 図 12 に示す SAM ユニット 9 a, 9 b の CPU 65 が、図 26 に示すステップ ST 66 において、認証部 64 が認証手段が正当であると認証したか否かを判断し、正当であると認証したと判断した場合にはステップ ST 72 の処理に進み、そうでない場合には処理を終了する（すなわち、処理に係わる権限を有しないと

判断し、処理を実行しない)。

ステップST72:

SAMユニット9a, 9bのCPU65が、復号鍵データを用いて、管理装置20から入力した暗号化されたデータ(暗号化データ)を、上記第2の暗号アルゴリズムに対応した第2の復号アルゴリズムで復号する。

そして、SAMユニット9a, 9bが、上記復号データが、適切に復号されたものであるか否かを判断し、適切に復号されたものであると判断した場合には、当該復号データを有効なものとして用いて、オナカード72等に許可した上記相互認証鍵データに関連付けられた処理を実行する。

10 一方、SAMユニット9a, 9bが、上記復号データが適切に復号されたものではないと判断した場合には、当該復号データを破棄(無効化)する。

以上説明したように、通信システム1によれば、管理装置20とSAMユニット9a, 9bとの間の相互認証と、管理装置20からSAMユニット9aに出力する暗号化データの生成とを異なる鍵データを用いて行うため、相互認証により用いた縮退鍵データが第三者によって不正に取得された場合でも、暗号化データは暗号鍵データを用いて暗号化されているため、当該第三者は当該暗号化データを解読できない。そのため、暗号化データを適切に保護できる。

また、通信システム1によれば、相互認証と暗号化データの生成とで異なる暗号・復号アルゴリズムを用いることで、相互認証で用いた暗号・復号アルゴリズムが第三者に漏れた場合でも、暗号化データは他の暗号アルゴリズムで暗号化されているため、当該第三者は解読できない。

また、管理装置20によれば、図16および図20等を用いて説明したように、SAMユニット9a, 9bに係わる処理に関連付けられた複数の相互認証鍵データを用いて縮退処理を行い、縮退鍵データを生成する。

25 そして、オナカード72やユーザカード73に、当該縮退鍵データ、並びにその生成に用いた相互認証鍵データを特定するための鍵指定データを書き込む。

また、オーナーカード72等を用いた管理装置20とSAMユニット9a, 9bとの間で、図25～図27を用いた相互認証を行うことで、SAMユニット9aが管理装置20から受けた鍵指定データを基に縮退鍵データを生成し、当該縮退鍵データが管理装置20が保持するものと一致した場合に、被認証手段である管

5 理装置20の正当性を確認できる。

また、その確認と共に、鍵指定データによって指定された相互認証鍵データに関連付けられた処理を、管理装置20に許可された処理であると判断できる。

そのため、認証手段であるSAMユニット9a, 9bは、従来のように全ての被認証手段（例えば、オーナーカード72およびユーザカード73を用いた管理装
10 置20等）に対応した相互認証鍵データを保持する必要がなく、しかも、被認証手段に許可した処理を管理テーブルで管理する必要もなく、処理負担が軽減される。

本発明は上述した実施形態には限定されない。

本発明は、例えば、オーナーカード72、ユーザカード73、トランスポートカード74およびAP暗号化カード75の何れかのカードのICに、そのカードの
15 使用者の生体情報を記憶させ、SAMユニット9a, 9bが、上述した相互認証と共に、当該カードに記憶された生体情報をさらに用いて、その使用者の正当性を認証してもよい。

例えば、上述した実施形態では、SAMユニット9a, 9bが管理装置20と
20 相互認証を行う場合を例示したが、SAMユニット9a, 9bがASPサーバ装置19a, 19bや他のSAMユニットなどの被認証手段と認証を行ってもよい。この場合には、当該被認証手段が、上述した縮退鍵データおよび鍵指定データを保持する。

また、上述した実施形態では、オーナーカード72およびユーザカード73が、
25 上述した縮退鍵データおよび鍵指定データを保持する場合を例示したが、その他の携帯装置などに、これらのデータを保持させてもよい。

産業上の利用可能性

本発明は、認証結果を基に所定の処理を行うデータ処理システムに適用可能である。

請 求 の 範 囲

1. 第1のデータ処理装置が第1の認証鍵データおよび暗号鍵データを保持し、第2のデータ処理装置が前記第1の認証鍵データに対応した第2の認証鍵データと前記暗号鍵データに対応した復号鍵データとを保持する場合に、前記第1のデータ処理装置と前記第2のデータ処理装置とが行うデータ処理方法であって、

前記第1のデータ処理装置が前記第1の認証鍵データを用い、前記第2のデータ処理装置が前記第2の認証鍵データを用いて、前記第1のデータ処理装置と前記第2のデータ処理装置との間で認証を行う第1の工程と、

前記第2のデータ処理装置が、前記第1の工程の前記認証により前記第1のデータ処理装置の正当性を認めた場合に、前記第1のデータ処理装置が前記暗号鍵データを用いて暗号化を行って前記第2のデータ処理装置に提供した暗号化データを、前記復号鍵データを用いて復号する第2の工程と、

前記第2のデータ処理装置が、前記第2の工程の前記復号によって得た復号データが適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる第3の工程と

を有するデータ処理方法。

2. 前記第1の工程において、前記第1のデータ処理装置および前記第2のデータ処理装置が、第1の暗号化アルゴリズム並びに前記第1の暗号化アルゴリズムに対応した第1の復号アルゴリズムを基に、所定のデータの暗号化および復号を行って前記認証を行い、

前記第2の工程において、前記第2のデータ処理装置が、第2の暗号化アルゴリズムを基に暗号化された前記暗号化データを、前記第2の暗号化アルゴリズムに対応した第2の復号アルゴリズムを基に前記復号する

請求項1に記載のデータ処理方法。

3. 前記第2の工程において、前記第2のデータ処理装置が、前記第1の工

程の前記認証により、前記第 1 の認証鍵データと前記第 2 の認証鍵データとが同じであると判断した場合に、前記第 1 のデータ処理装置の正当性を認める

請求項 1 に記載のデータ処理方法。

4. 前記第 1 の認証鍵データが所定の鍵データを用いて所定の生成方法で生成されている場合に、

前記第 1 の工程は、

前記第 1 のデータ処理装置が、前記第 1 の認証鍵データの生成に用いられた鍵データを指定する鍵指定データを前記第 2 のデータ処理装置に提供する第 4 の工程と、

10 前記第 2 のデータ処理装置が、前記第 4 の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で前記第 2 の認証鍵データを生成する第 5 の工程と、

前記第 1 のデータ処理装置が前記第 1 の認証鍵データを用い、前記第 2 のデータ処理装置が前記第 5 の工程で生成した前記第 2 の認証鍵データを用いて、
15 前記認証を行う第 6 の工程と、

前記第 2 のデータ処理装置が、前記第 6 の工程の前記認証により、前記第 1 の認証鍵データと前記第 2 の認証鍵データとが同じであると判断すると、前記第 1 のデータ処理装置の正当性を認める第 7 の工程と

を有する請求項 1 に記載のデータ処理方法。

20 5. 第 1 の認証鍵データおよび暗号鍵データを保持する第 1 のデータ処理装置と、

前記第 1 の認証鍵データに対応した第 2 の認証鍵データと前記暗号鍵データに対応した復号鍵データとを保持する第 2 のデータ処理装置と

を有し、

25 前記第 1 のデータ処理装置が、前記第 1 の認証鍵データを用い、前記第 2 のデータ処理装置が前記第 2 の認証鍵データを用いて、前記第 1 のデータ処理

装置と前記第 2 のデータ処理装置との間で認証を行い、

前記第 2 のデータ処理装置が、前記認証により前記第 1 のデータ処理装置の正当性を認めた場合に、前記第 1 のデータ処理装置が前記暗号鍵データを用いて暗号化を行って前記第 2 のデータ処理装置に提供した暗号化データを、前記
5 復号鍵データを用いて復号し、

前記第 2 のデータ処理装置が、前記復号によって得た復号データが適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる データ処理システム。

6. 認証鍵データおよび暗号鍵データを保持するデータ処理装置が行うデータ
10 処理方法であって、

前記認証鍵データを用いて、認証先と認証を行う第 1 の工程と、

前記第 1 の工程の前記認証の後に、前記暗号鍵データを用いて所定のデータを暗号化する第 2 の工程と、

前記第 2 の工程の前記暗号化により得られたデータを前記認証先に出力
15 する第 3 の工程と

を有するデータ処理方法。

7. 鍵データを保持する前記認証先の認証手段が、第 1 の認証鍵データを保持する前記データ処理装置から指定された前記鍵データを用いて所定の生成手法を基に第 2 の認証鍵データを生成し、前記第 2 の認証鍵データを用いて前記データ
20 処理装置と認証を行い、当該認証により、前記第 1 の認証鍵データと前記第 2 の認証鍵データとが同じであることを確認したことを条件に、前記第 3 の工程で出力された前記データを有効なものとして用いる場合に、

前記第 1 の工程は、

前記所定の生成方法を基に前記第 1 の認証鍵データを生成したときに用
25 いた前記鍵データを指定する鍵指定データを前記認証手段に提供する第 4 の工程と、

前記第 1 の認証鍵データを用いて、前記認証手段と前記認証を行う第 5
の工程と

を有する請求項 6 に記載のデータ処理方法。

5 8. 所定のデータを暗号化して認証先に出力するデータ処理装置であって、
認証鍵データおよび暗号鍵データを記憶する記憶手段と、
前記認証鍵データを用いて、認証先と認証を行う認証手段と、
前記認証手段の前記認証の後に、前記暗号鍵データを用いて所定のデー
タを暗号化する暗号化手段と、

10 前記暗号化手段の前記暗号化により得られたデータを前記認証先に出力
する出力手段と

を有するデータ処理装置。

9. 認証鍵データおよび暗号鍵データを保持するデータ処理装置が実行する
プログラムであって、

15 前記認証鍵データを用いて、認証先と認証を行う第 1 の手順と、
前記第 1 の手順の前記認証の後に、前記暗号鍵データを用いて所定のデ
ータを暗号化する第 2 の手順と、

前記第 2 の手順の前記暗号化により得られたデータを前記認証先に出力
する第 3 の手順と

を有するプログラム。

20 10. 認証鍵データおよび復号鍵データを保持するデータ処理装置が行うデー
タ処理方法であって、

前記認証鍵データを用いて、被認証手段と認証を行う第 1 の工程と、

前記復号鍵データを用いて、前記被認証手段から受けたデータを復号す
る第 2 の工程と、

25 前記第 1 の工程の前記認証により前記被認証手段の正当性を認めると、
前記第 2 の工程の前記復号により得られたデータを有効なものとして用いる第 3

の工程と

を有するデータ処理方法。

11. 所定の鍵データを保持する前記データ処理装置が、前記鍵データを用いて所定の生成手法で生成され前記鍵データを復元困難な第1の認証鍵データを保

5 持する前記被認証手段と認証を行う場合に、

前記第1の工程は、

前記鍵データを指定する鍵指定データを前記被認証手段から受ける第4の工程と、

10 前記第4の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で第2の認証鍵データを生成する第5の工程と、

前記第5の工程で生成した前記第2の認証鍵データを用いて、前記第1の認証鍵データを前記認証に用いる前記被認証手段と前記認証を行う第6の工程と、

15 前記第6の工程の前記認証により、前記第1の認証用データと前記第2の認証用データとが同じであると判断した場合に、前記被認証手段の正当性を認める第7の工程と

を有する請求項10に記載のデータ処理方法。

20 12. 前記第3の工程において、前記鍵データに関連付けられた、前記被認証手段に許可されたデータ処理装置の機能、または前記データ処理装置が保持するデータへのアクセスを実行する

請求項10に記載のデータ処理方法。

13. 認証鍵データおよび復号鍵データを保持するデータ処理装置であって、前記認証鍵データを用いて、被認証手段と認証を行う認証手段と、前記被認証手段からデータを入力する入力手段と、

25 前記復号鍵データを用いて、前記入力手段を介して前記被認証手段から入力した前記データを復号する復号手段と、

前記認証手段の前記認証により前記被認証手段の正当性を認めると、前記復号手段の前記復号により得られたデータを有効なものとして用いる制御手段と

を有するデータ処理装置。

- 5 14. 認証鍵データおよび復号鍵データを保持するデータ処理装置が実行するプログラムであって、

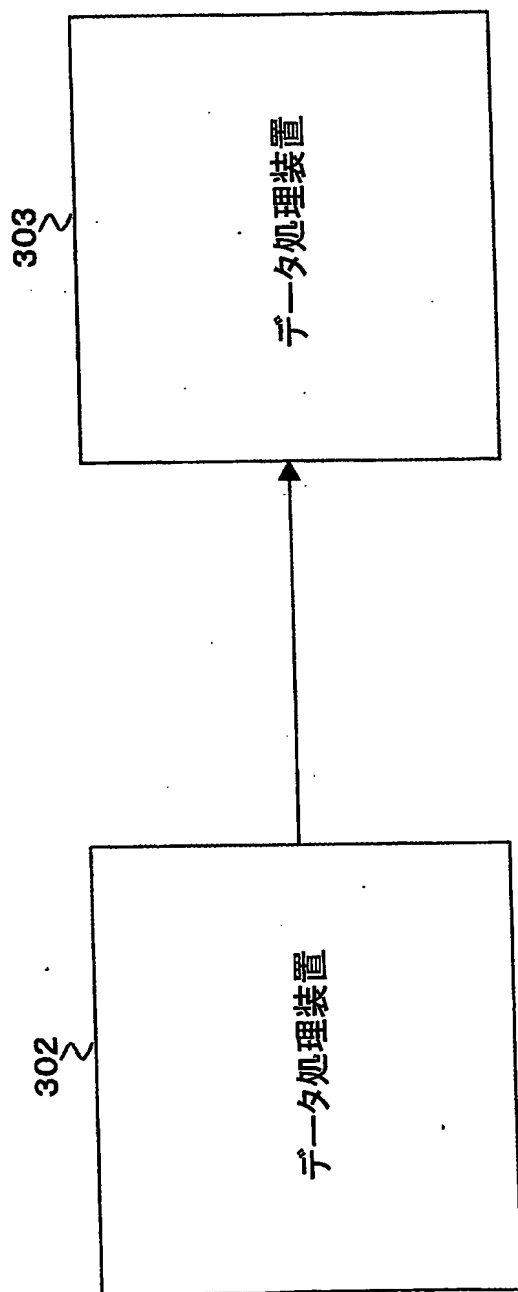
前記認証鍵データを用いて、被認証手段と認証を行う第1の手順と、

前記復号鍵データを用いて、前記被認証手段から受けたデータを復号する第2の手順と、

- 10 前記第1の手順の前記認証により前記被認証手段の正当性を認めると、前記第2の手順の前記復号により得られたデータを有効なものとして用いる第3の手順と

を有するプログラム。

FIG. 1



301

FIG. 2

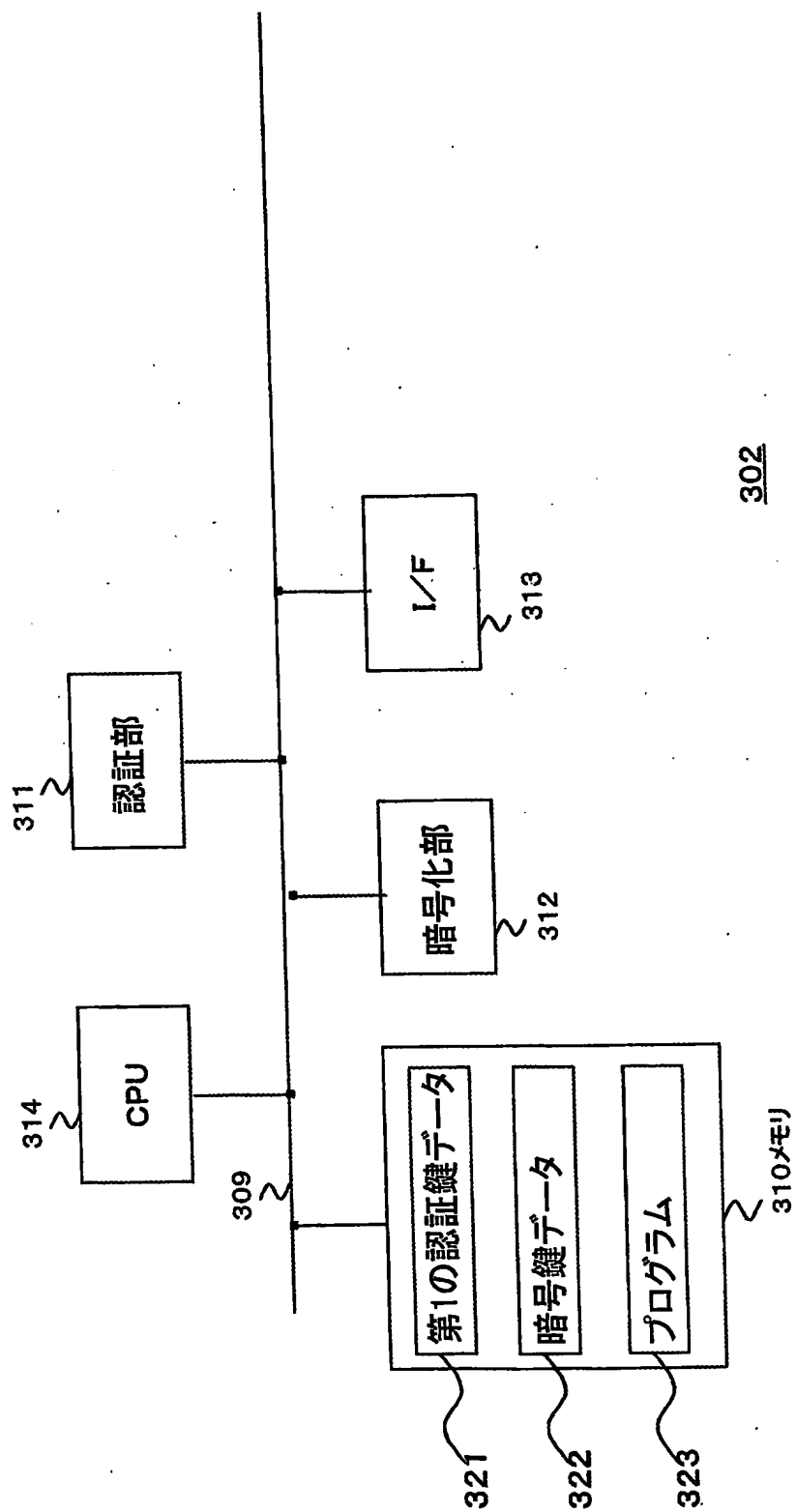


FIG. 3

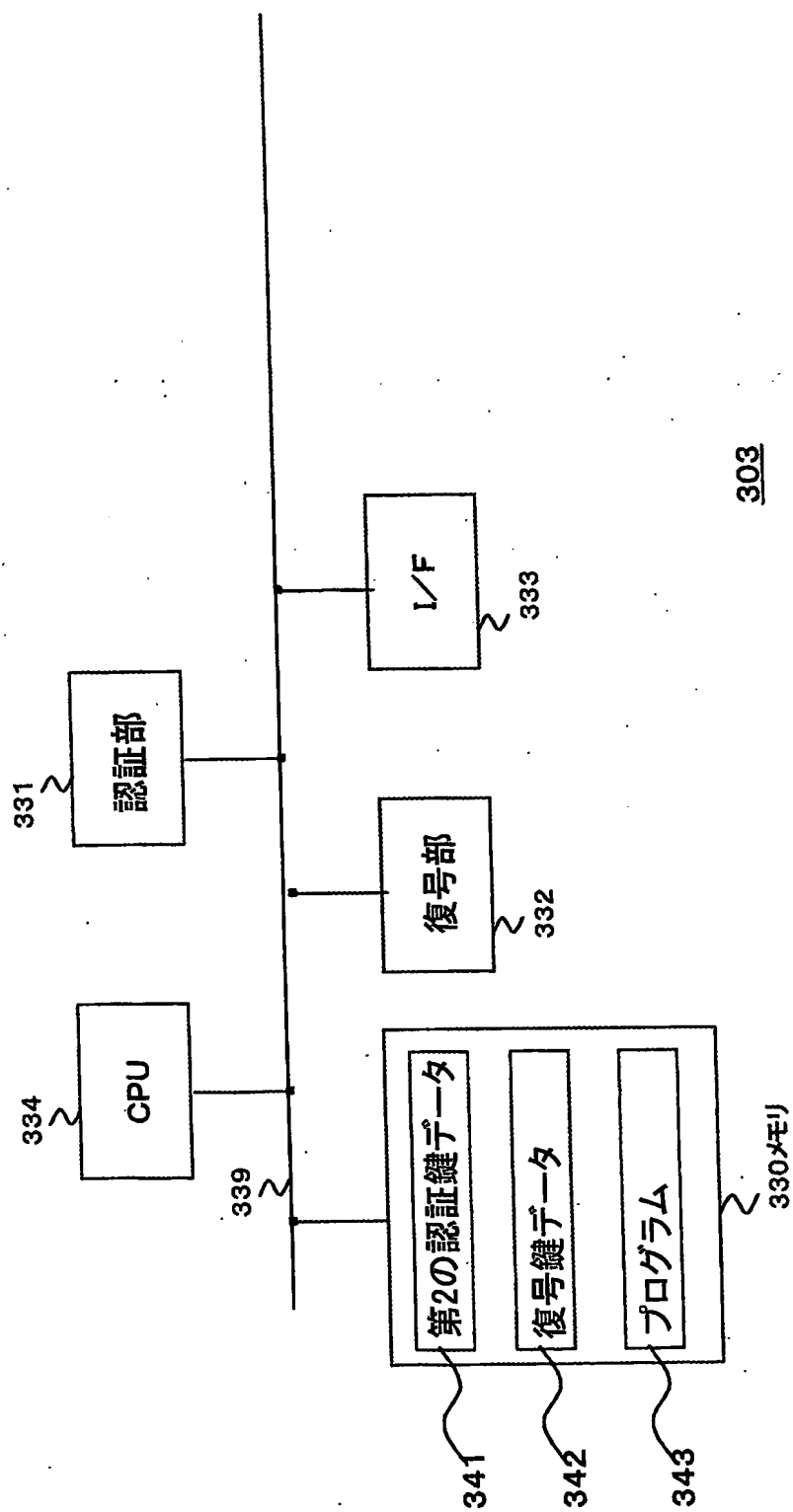


FIG. 4

データ処理装置303

データ処理装置302

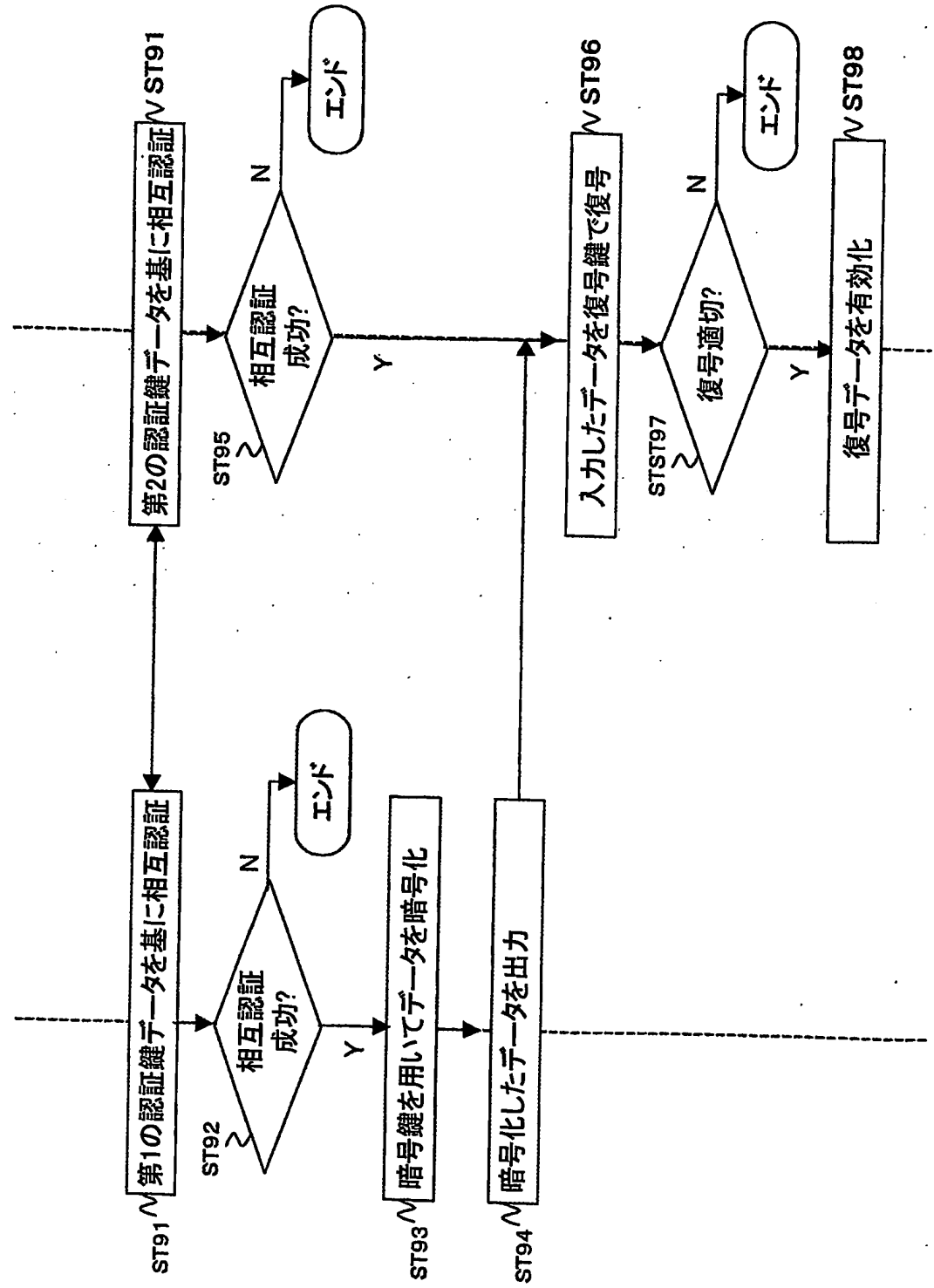


FIG. 5

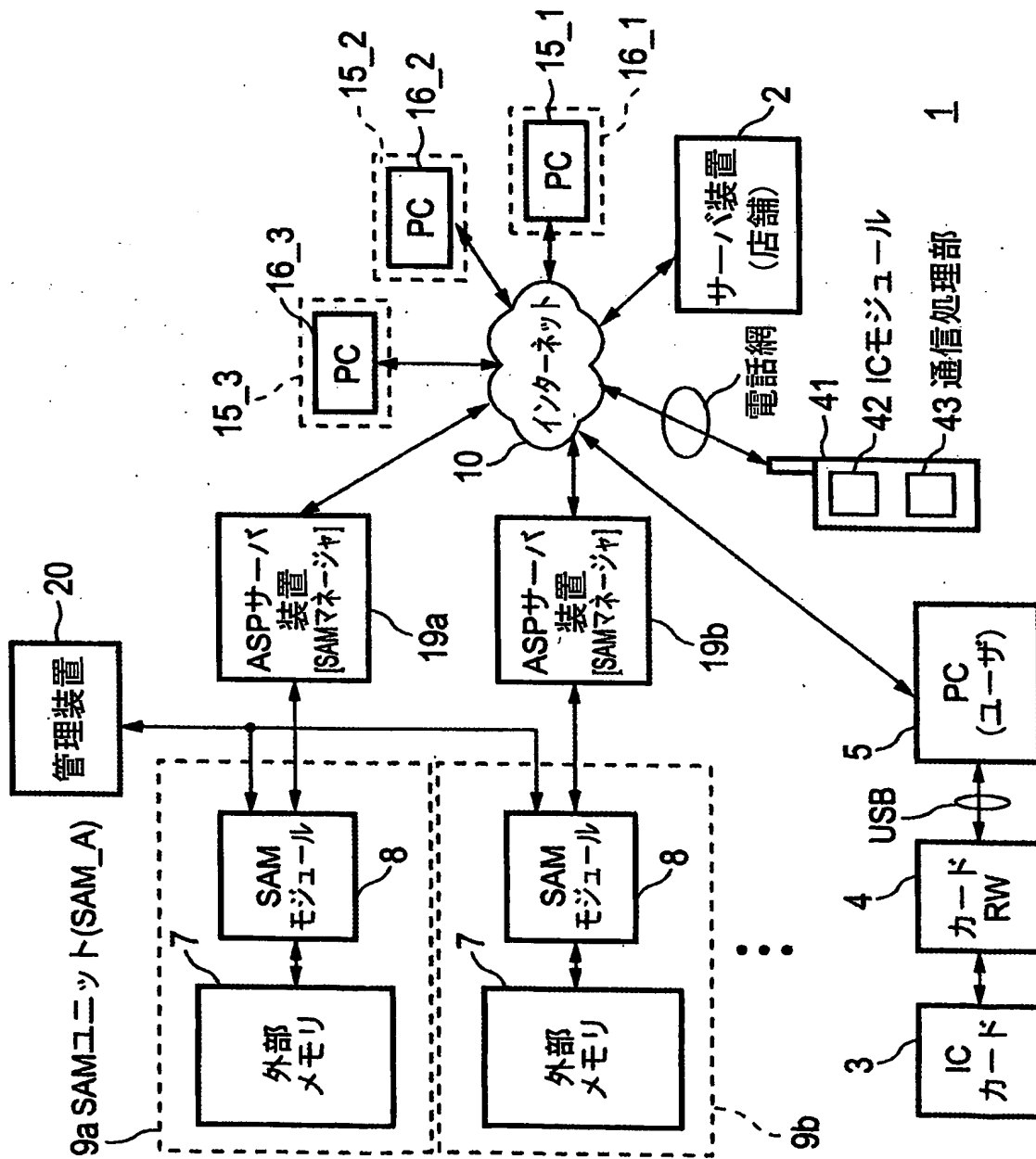


FIG. 6

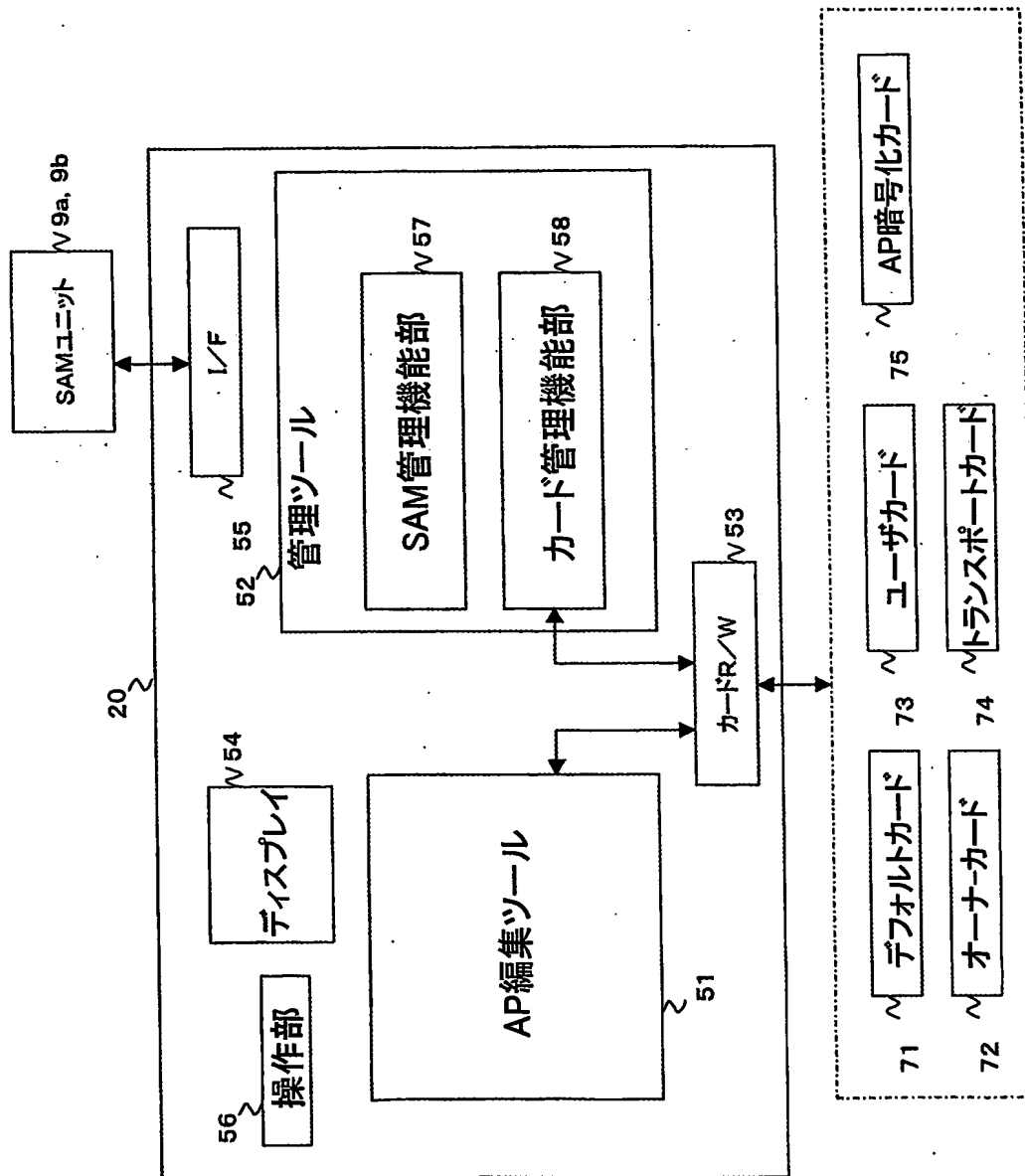


FIG. 7

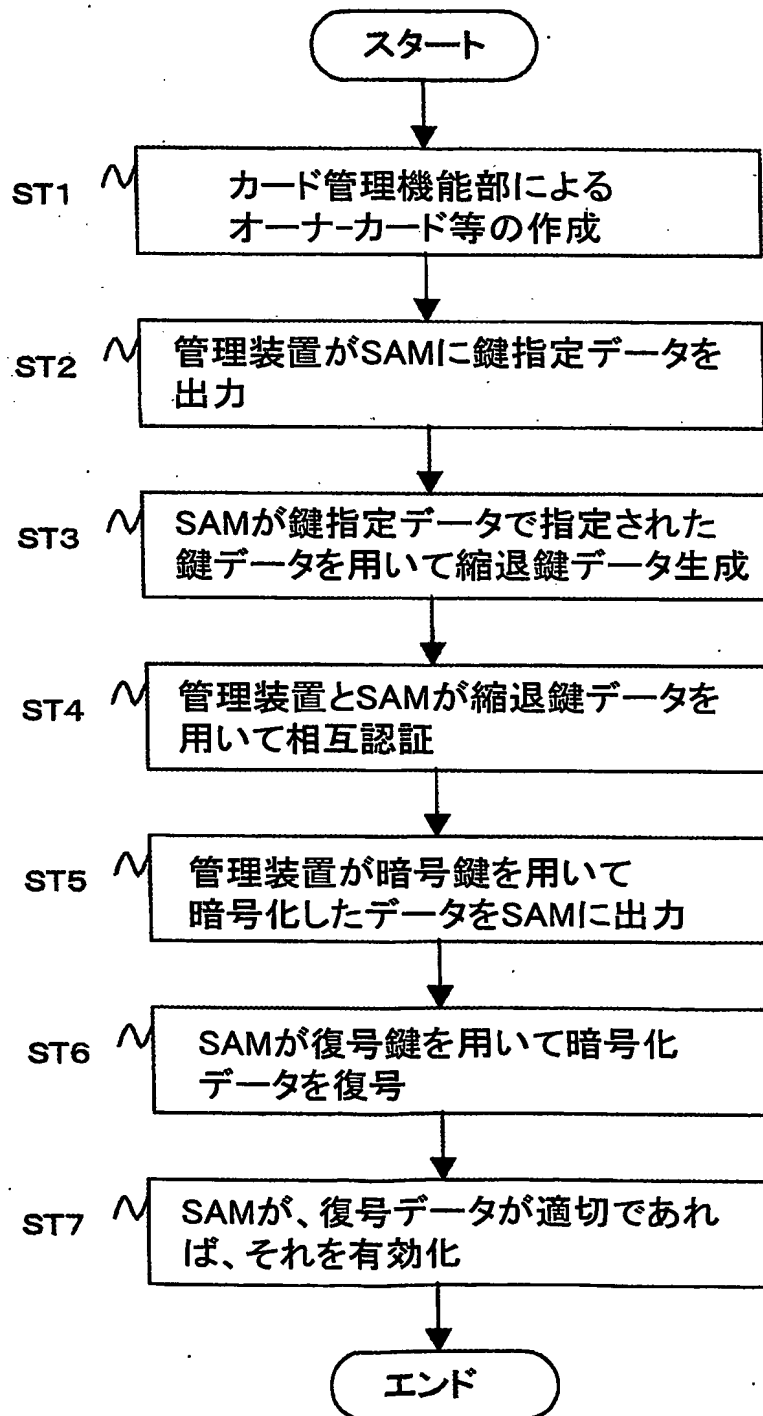


FIG. 8

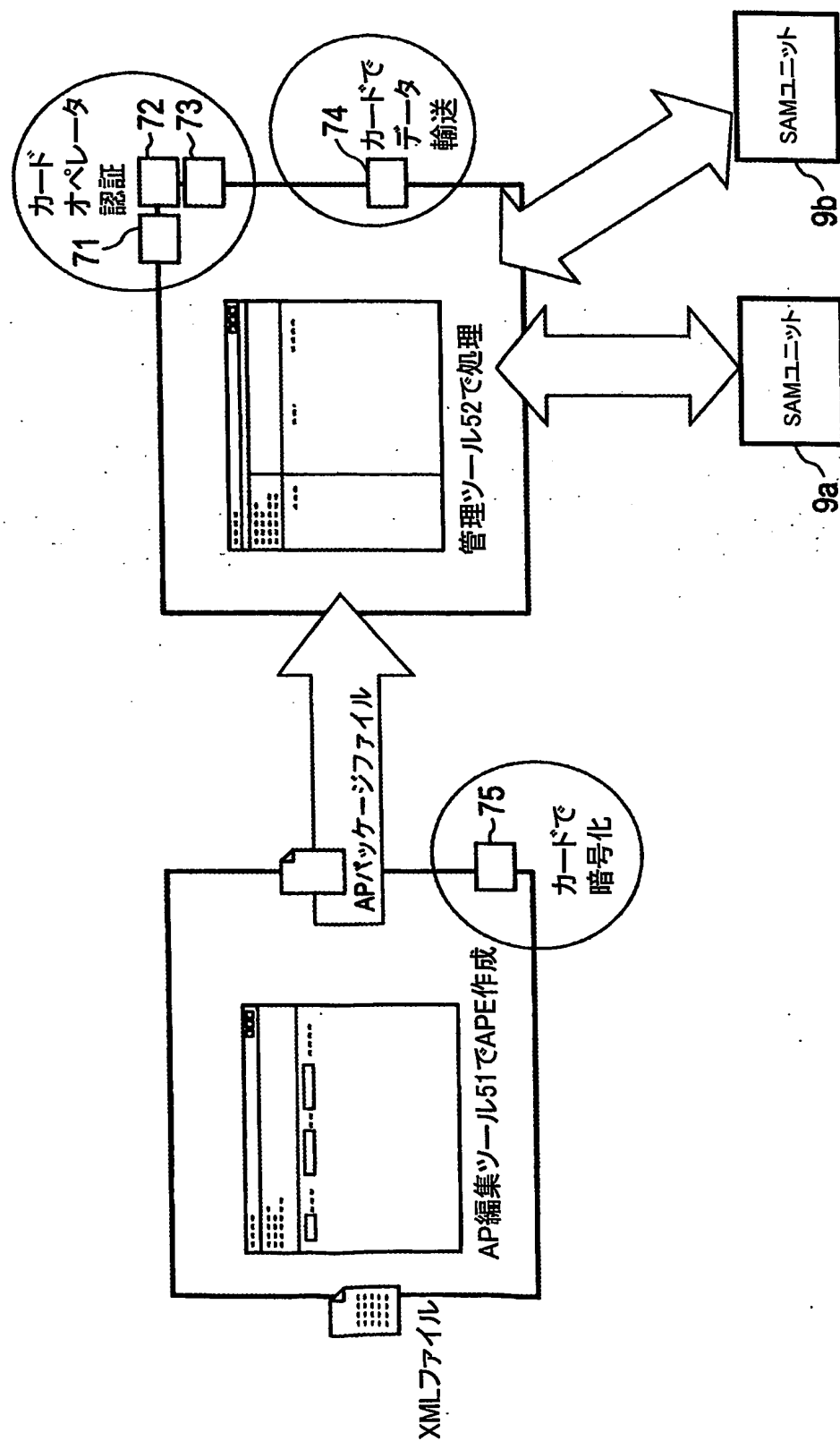


FIG. 9

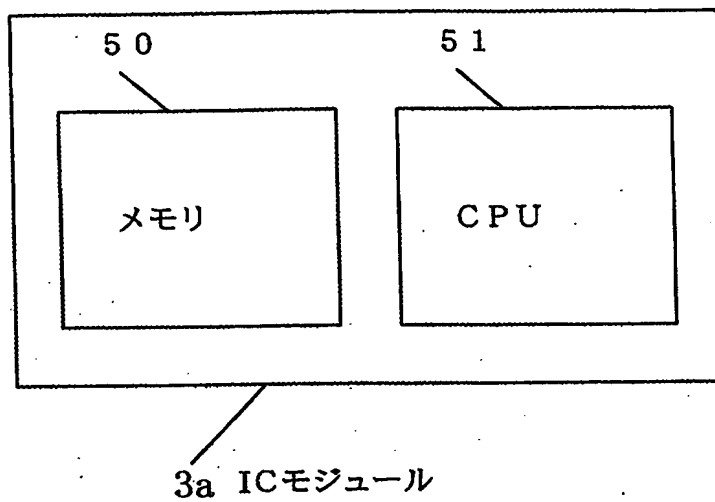


FIG. 10

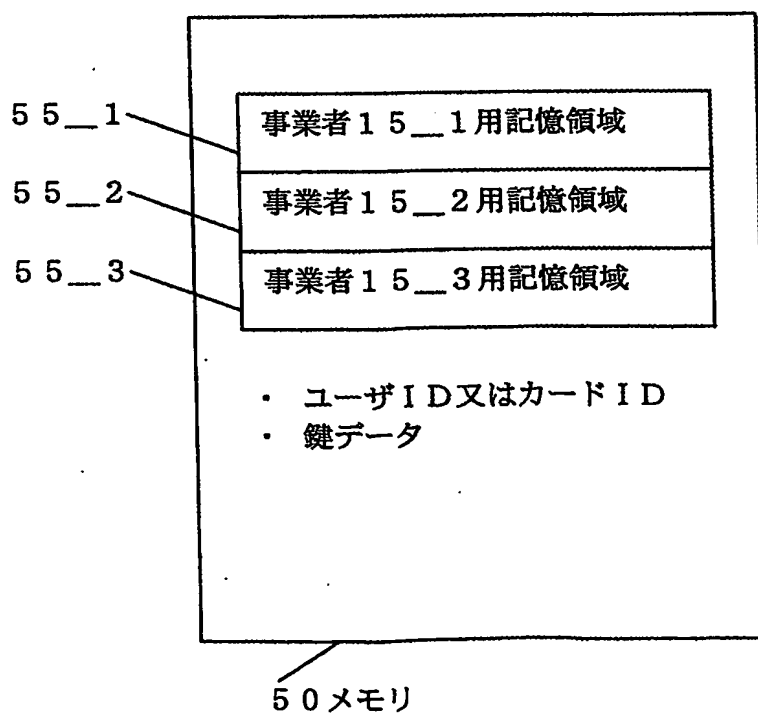


FIG. 11

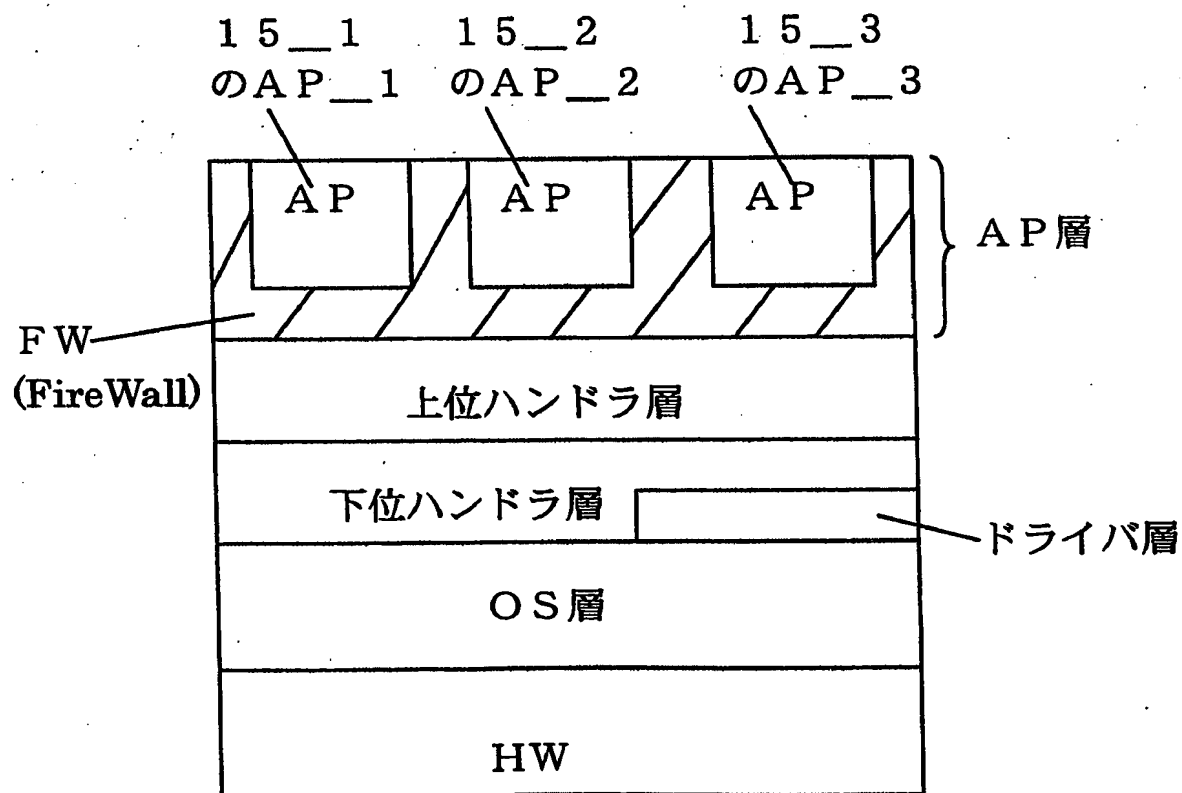


FIG. 12

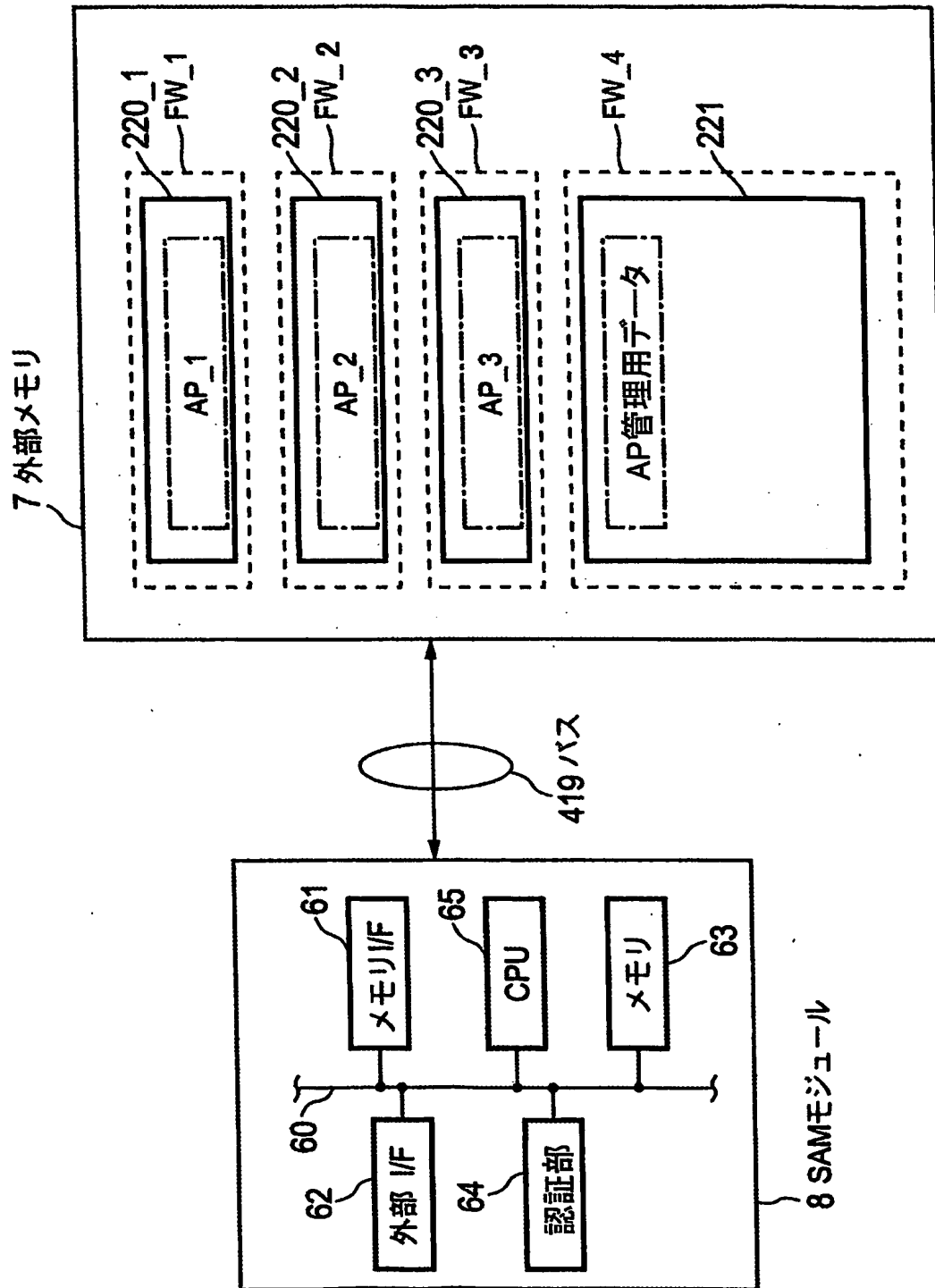


FIG. 13

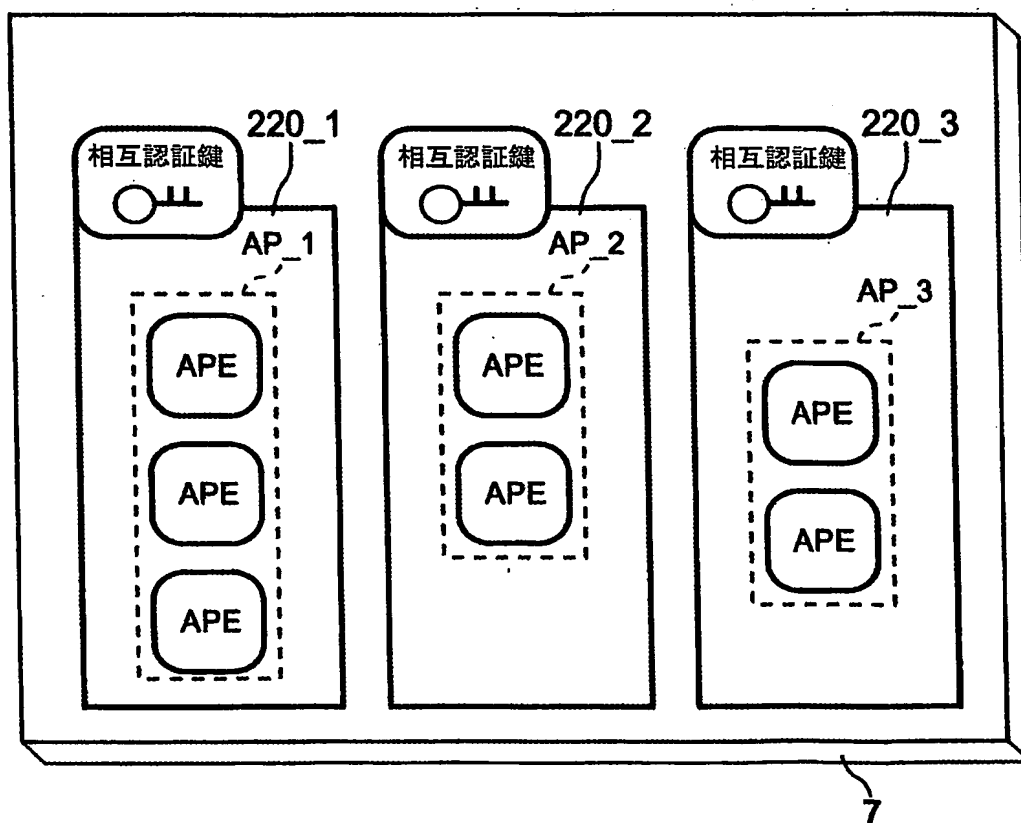


FIG. 14

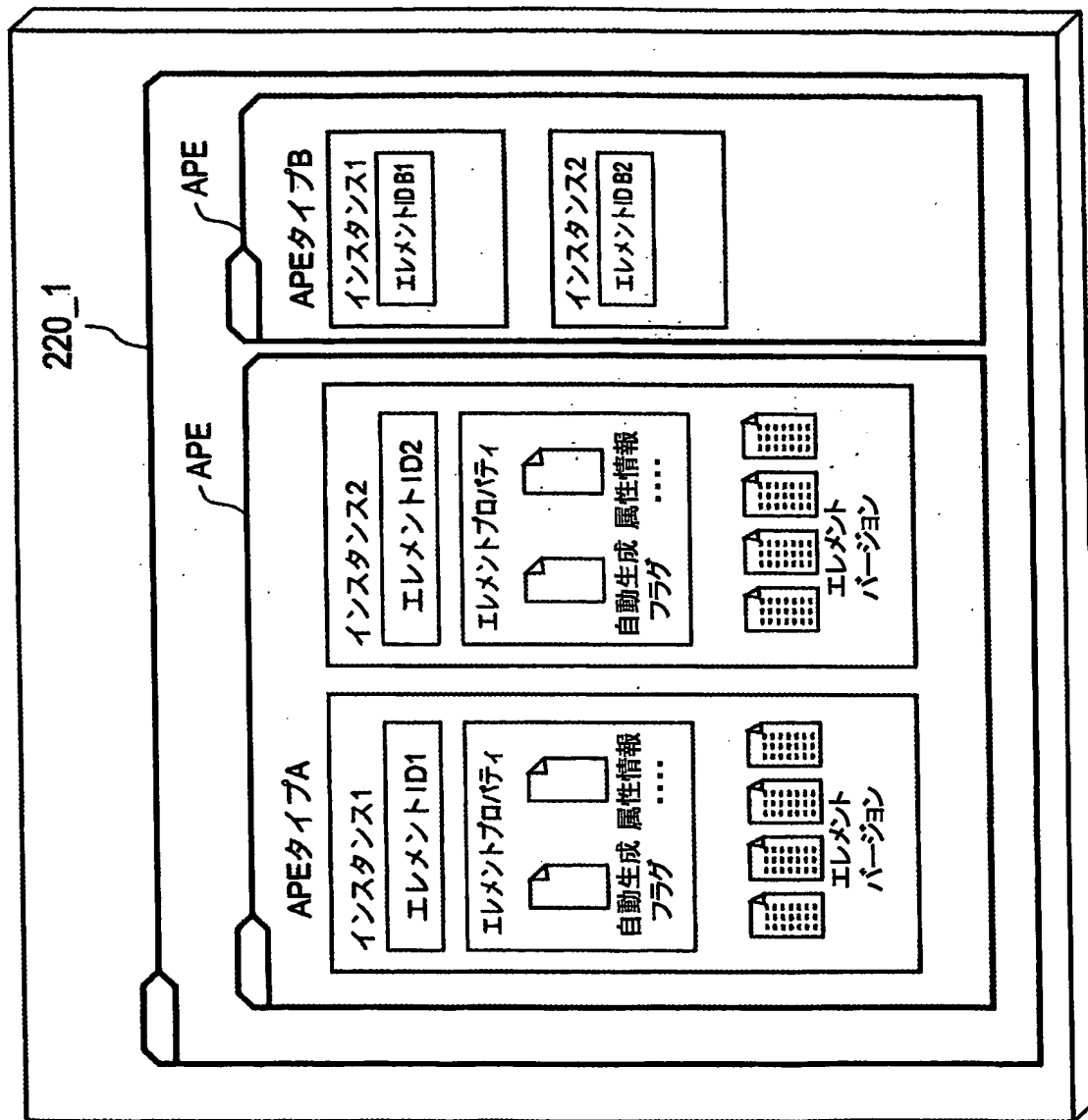


FIG. 15

APE タイプ番号	APEタイプ
...	ICシステム鍵
...	ICエリア鍵
...	ICサービス鍵
...	IC縮退鍵
...	IC鍵変更パッケージ
...	IC発行鍵パッケージ
...	IC拡張発行鍵パッケージ
...	ICエリア登録鍵パッケージ
...	ICエリア削除鍵パッケージ
...	ICサービス登録鍵パッケージ
...	ICサービス削除鍵パッケージ
...	ICメモリ分割鍵パッケージ
...	ICメモリ分割素鍵パッケージ
...	障害記録ファイル
...	相互認証用鍵
...	パッケージ鍵
...	ネガリスト
...	サービスデータテンポラリファイル

FIG. 16

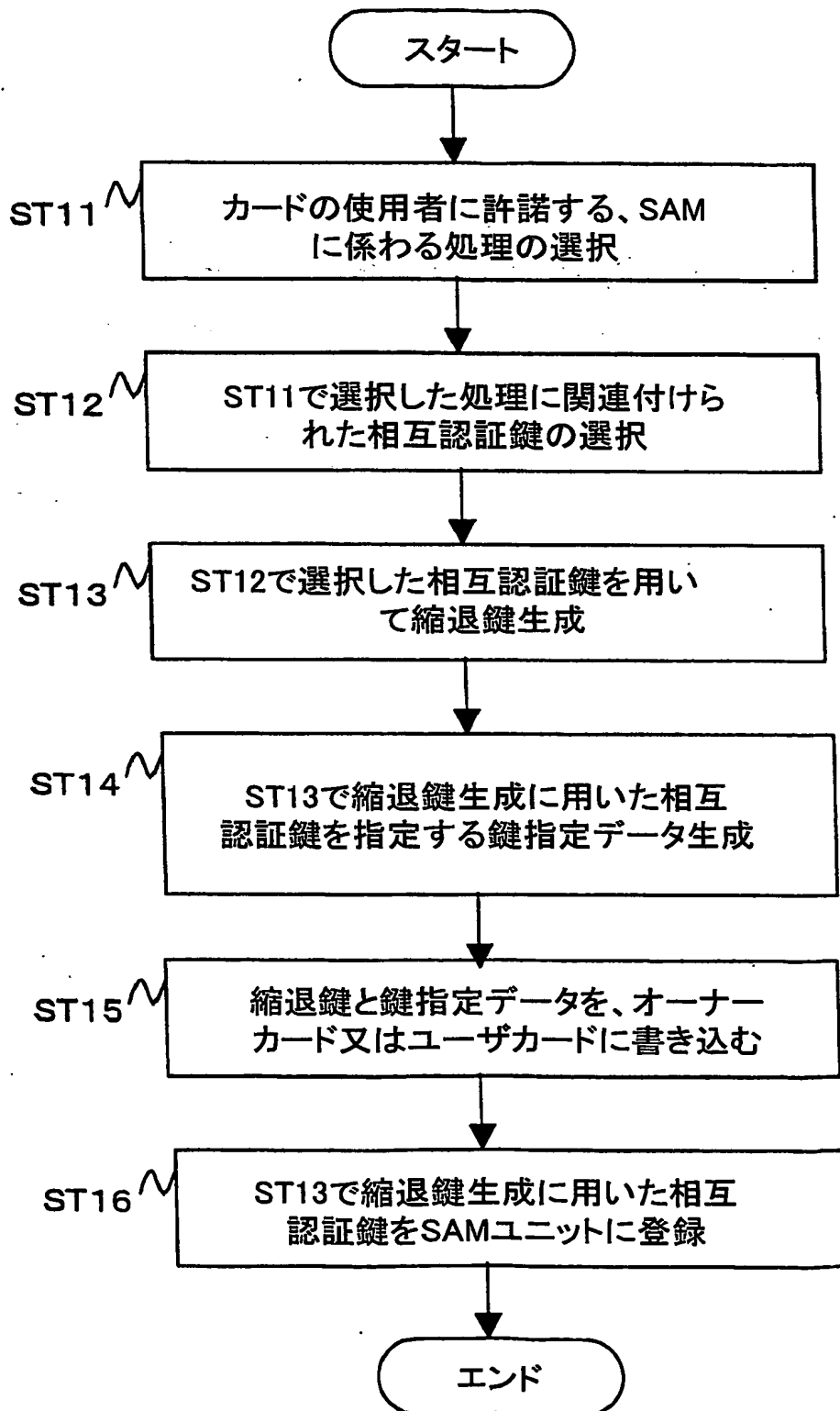


FIG. 17

相互認証鍵名	AP記憶領域・ID	APEタイプ 番号	インスタンス 番号	エレメント バージョン
デバイス鍵
ターミネーション鍵
製造設定サービス相互認証鍵
機器管理サービス相互認証鍵
通信管理サービス相互認証鍵
相互認証サービス相互認証鍵
AP記憶領域管理サービス 相互認証鍵
サービスAP・記憶領域 相互認証鍵
システムAP・記憶領域 相互認証鍵
製造者AP記憶領域 相互認証鍵

FIG. 18

AP記憶領域ID	エレメントタイプ番号	エレメント インスタンス番号	エレメント バージョン番号
2バイト	2バイト	2バイト	2バイト
所属する APIソース領域	相互認証鍵(固定値)	リリース鍵リングのID	使用する鍵の バージョン番号

相互認証鍵名	AP記憶領域ID	APE タイプ番号	インスタンス番号	エレメント バージョン番号
デバイス鍵
機器管理サービス相互認証鍵
通信管理サービス相互認証鍵
AP記憶領域管理 サービス相互認証鍵
サービスAP記憶領域 AP-R相互認証鍵
ターミネーション鍵

FIG. 19A

・実行可能なコマンド

サービス種別	コマンド名
機器管理サービス	...
通信管理サービス	...
ICサービス	...
相互認証サービス	...
AP記憶領域管理サービス	...

FIG. 19B

FIG. 20

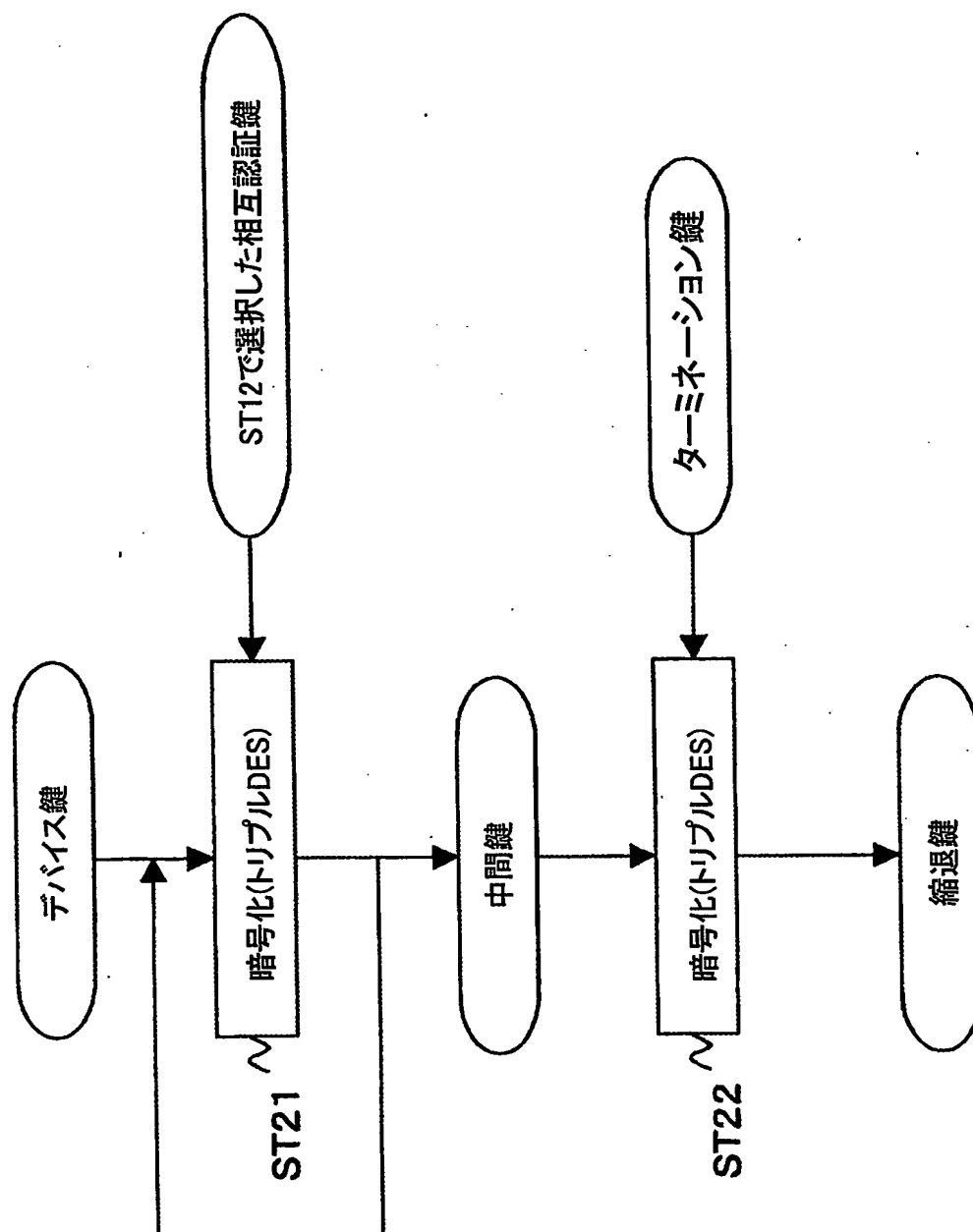


FIG. 21

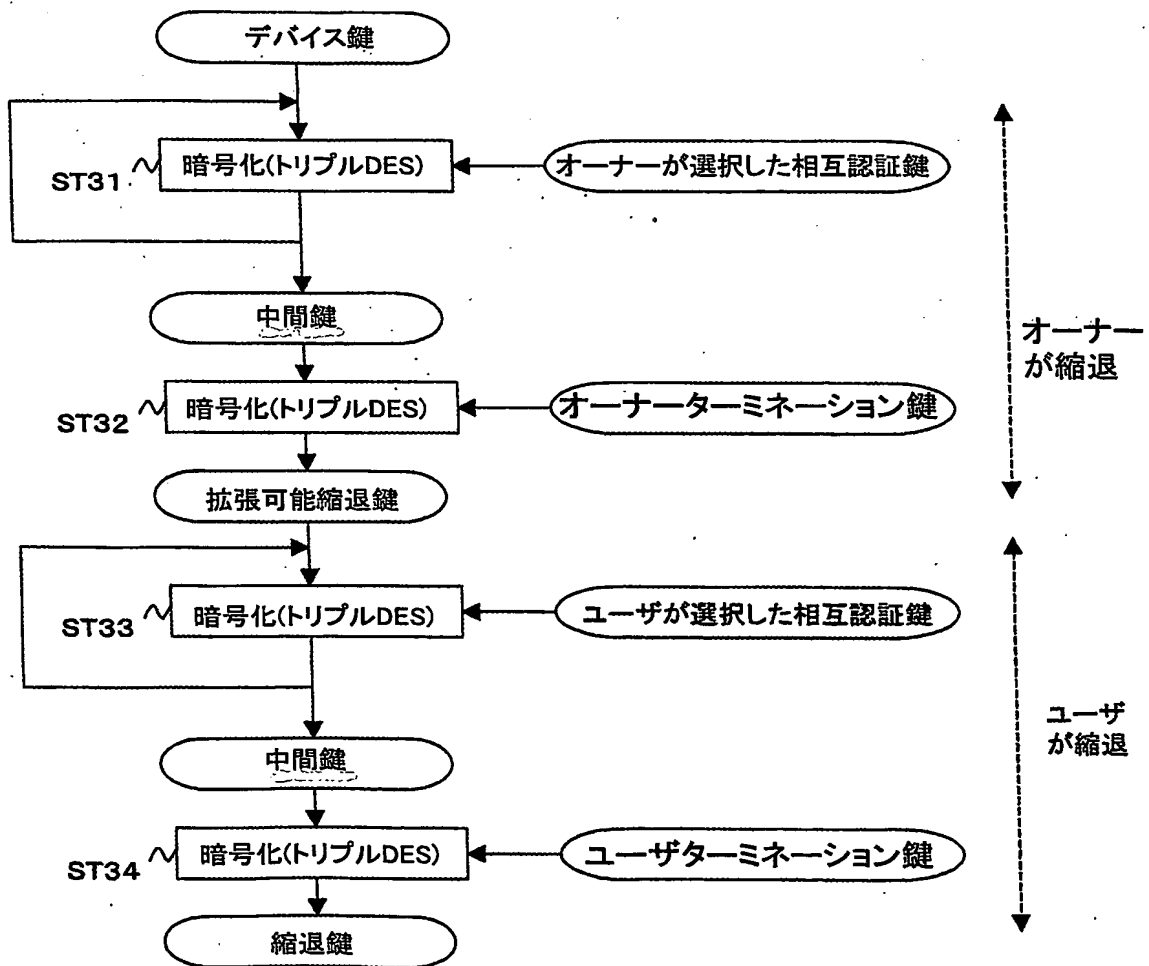


FIG. 22

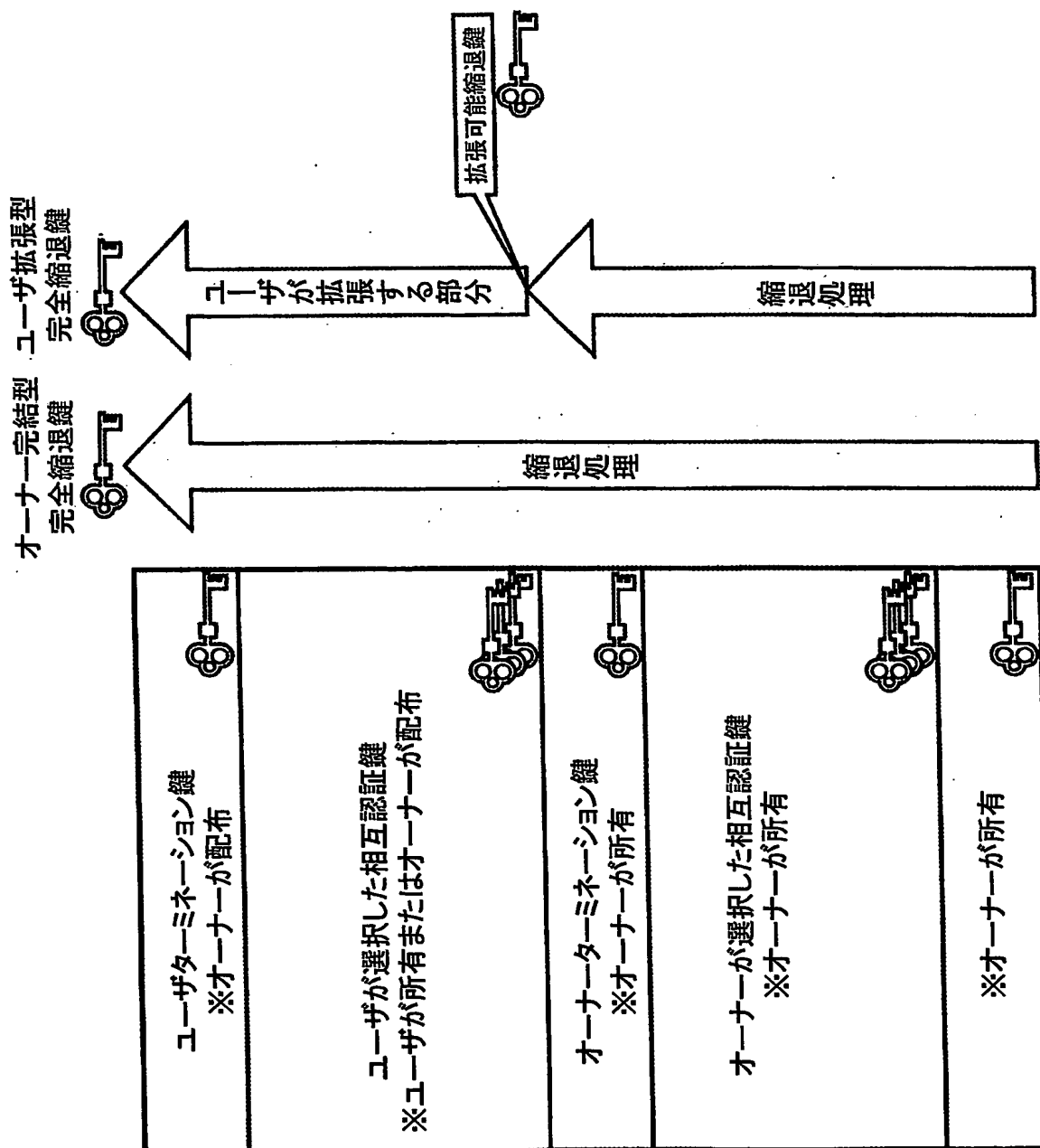


FIG. 23

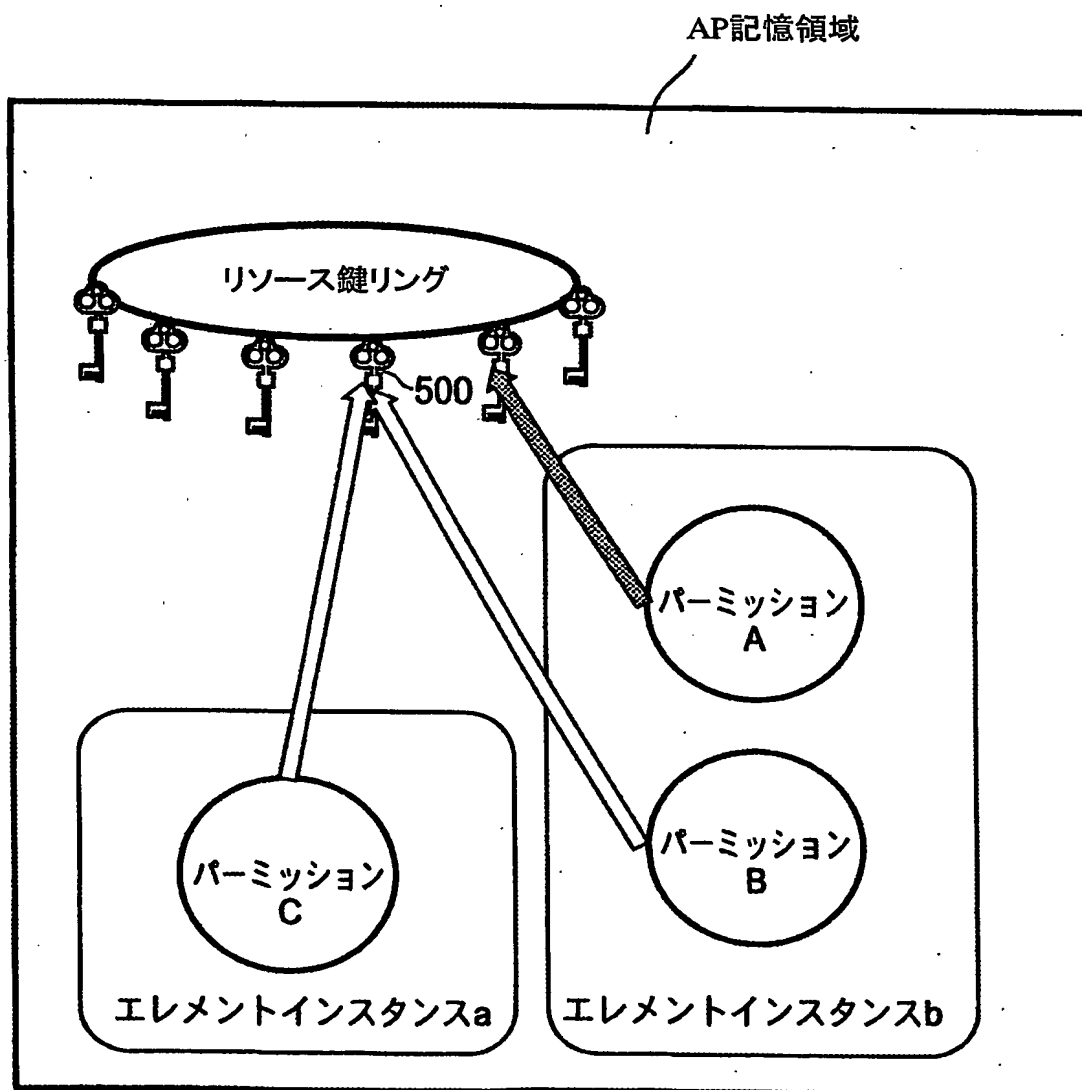


FIG. 24

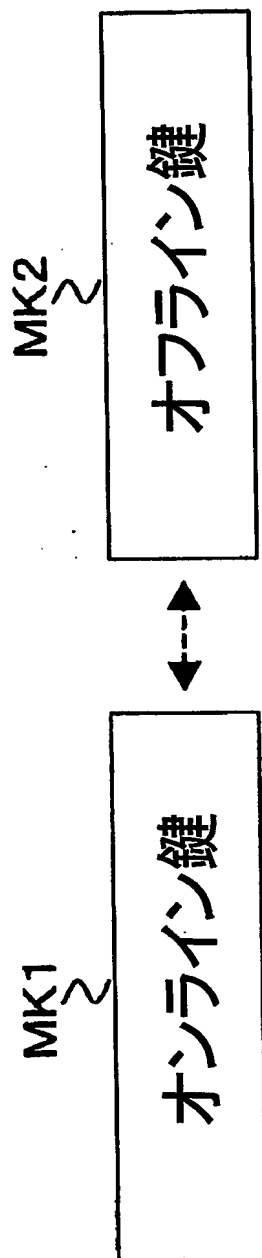


FIG. 25

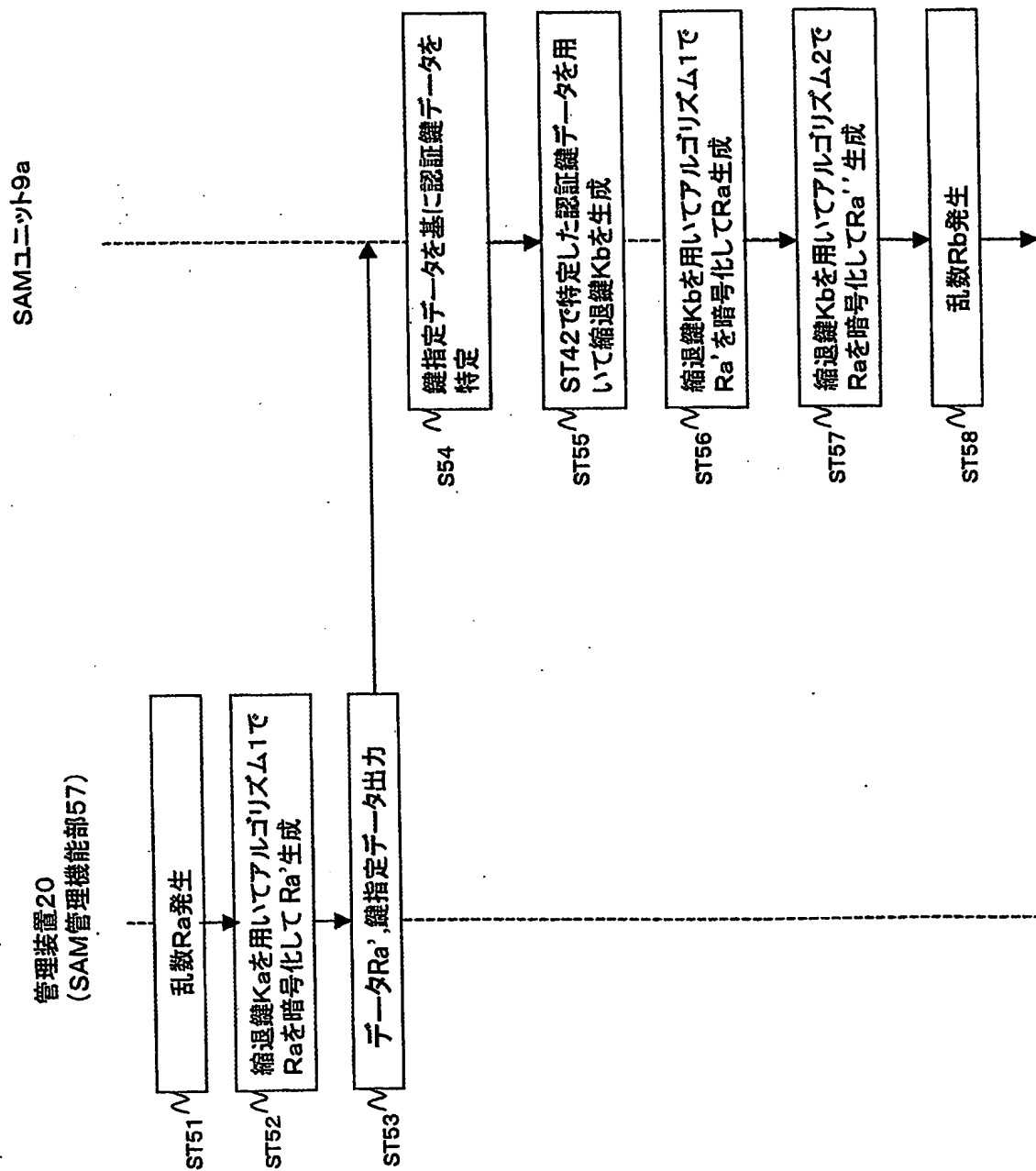


FIG. 26

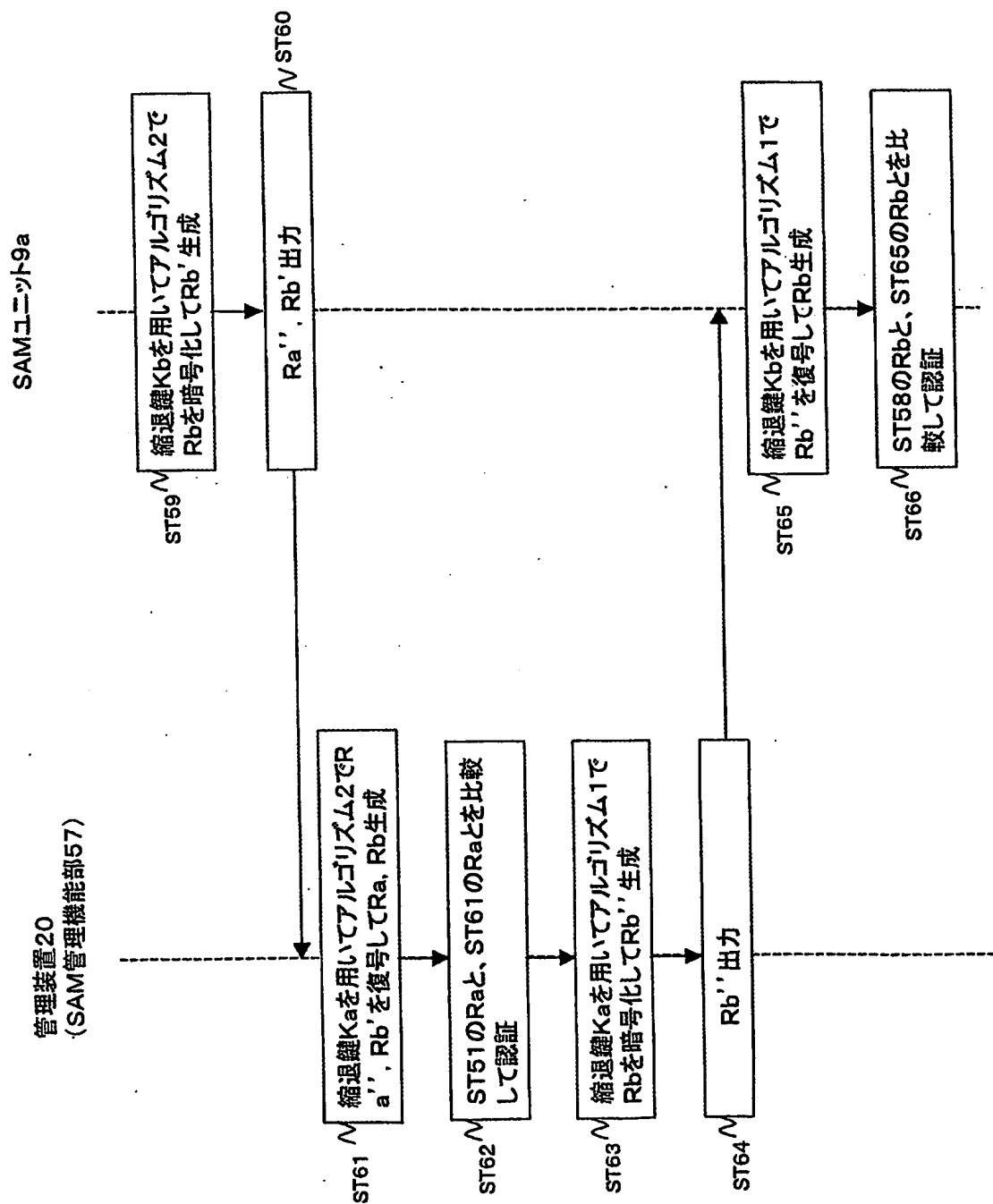
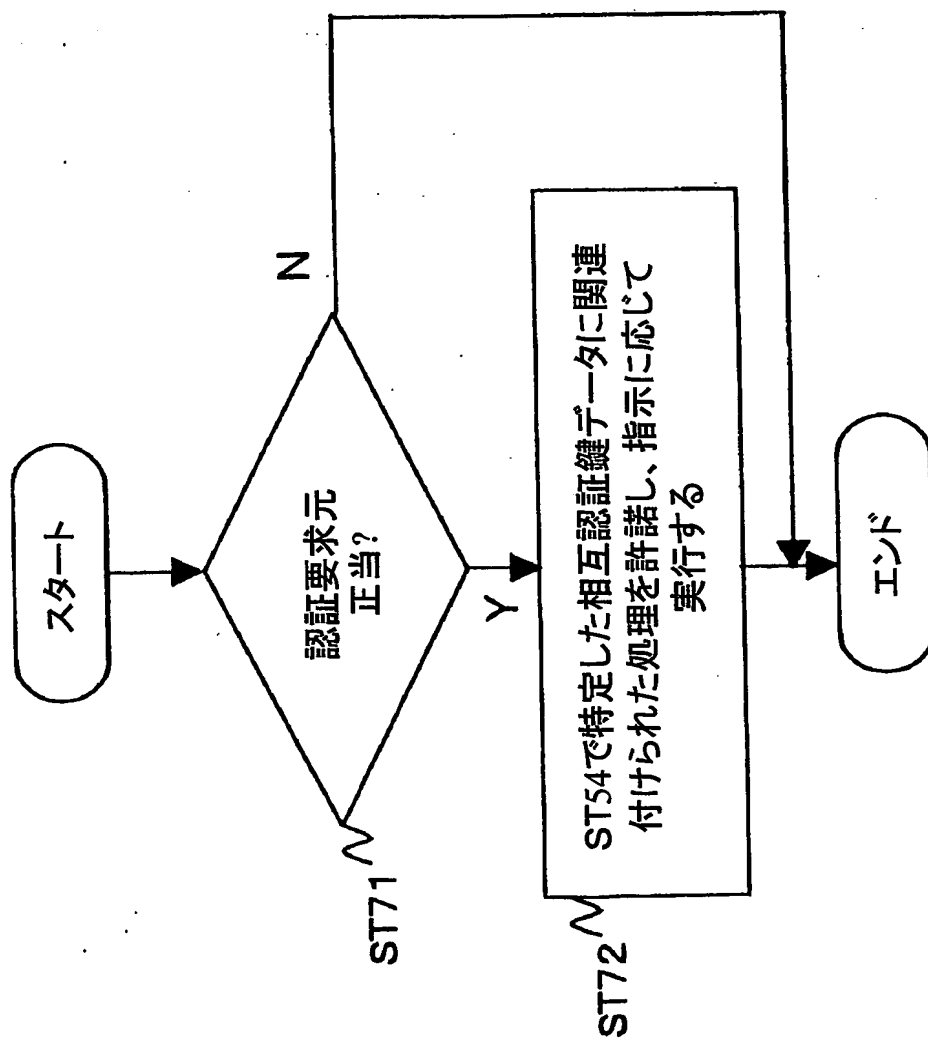


FIG. 27



符号の説明

- 1…通信システム
- 2…サーバ装置
- 3…ICカード
- 4…カードRW
- 6…PC
- 7…外部メモリ
- 8…SAMモジュール
- 9 a, 9 b…SAMユニット
- 19 a, 19 b…ASPサーバ装置
- 20…管理装置 51…AP編集ツール
- 52…管理ツール
- 53…カードリーダー・ライター
- 54…ディスプレイ
- 55…I/F
- 56…操作部
- 57…SAM管理機能部
- 58…カード管理機能部
- 61…メモリ I/F
- 62…外部 I/F
- 63…メモリ
- 64…認証部
- 65…CPU
- 71…デフォルトカード
- 72…オーナーカード

7 3...ユーザカード
7 4...トランスポートカード
7 5...A P 暗号化カード
3 0 1...データ処理システム
3 0 2, 3 0 3...データ処理装置
3 0 2, 3 1 0...メモリ
3 1 1...認証部
3 1 2...暗号化部
3 1 3...インタフェース
3 1 4...CPU
3 3 0...メモリ
3 3 1...認証部
3 3 2...復号部
3 3 3...I / F

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/11804

A. CLASSIFICATION OF SUBJECT MATTERInt.Cl.⁷ H04L9/08, H04L9/10, H04L9/32, G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.⁷ H04L9/08, H04L9/10, H04L9/32, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2000-332748 A (Sony Corp.), 30 November, 2000 (30.11.00),	6, 8, 9, 10, 13, 14
Y	Full text & EP 1037131 A	1-5, 7, 11, 12
X	JP 2002-111658 A (Sony Corp.), 12 April, 2002 (12.04.02),	6, 8, 9, 10, 13, 14
Y	Full text & EP 1176757 A	1-5, 7, 11, 12
X	JP 7-87078 A (Kabushiki Kaisha Roreru Intelligent Systems),	6, 8, 9, 10, 13, 14
Y	31 March, 1995 (31.03.95), Full text (Family: none)	1-5, 7, 11, 12

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"I" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
10 December, 2003 (10.12.03)Date of mailing of the international search report
24 December, 2003 (24.12.03)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/11804

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-327142 A (Sony Corp.), 08 December, 1998 (08.12.98), Full text & EP 867843 A	1-5, 7, 11, 12
X	JP 2000-332742 A (Sony Corp.), 30 November, 2000 (30.11.00), Full text & EP 1054314 A	6, 8, 9
A	JP 8-242224 A (Tatsuhiko MEYA), 17 September, 1996 (17.09.96), Full text (Family: none)	1-14

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08, H04L9/10, H04L9/32, G09C1/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08, H04L9/10, H04L9/32, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年

日本国公開実用新案公報 1971-2003年

日本国登録実用新案公報 1994-2003年

日本国実用新案登録公報 1996-2003年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y	JP 2000-332748 A (ソニー株式会社) 2000. 11. 30, 全文 & EP 1037131 A	6, 8, 9, 10, 13, 14 1-5, 7, 11, 12
X Y	JP 2002-111658 A (ソニー株式会社) 2002. 04. 12, 全文 & EP 1176757 A	6, 8, 9, 10, 13, 14 1-5, 7, 11, 12

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に関する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

10. 12. 03

国際調査報告の発送日

2003

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

石田 信行



5M

9469

電話番号 03-3581-1101 内線 3598

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 7-87078 A (株式会社ローレルインテリジェントシステムズ)	6, 8, 9, 10,
Y	1995. 03. 31, 全文 (ファミリーなし)	13, 14
Y	JP 10-327142 A (ソニー株式会社) 1998. 12. 08, 全文 & EP 867843 A	1-5, 7, 11, 12
X	JP 2000-332742 A (ソニー株式会社) 2000. 11. 30, 全文 & EP 1054314 A	1-5, 7, 11, 12
A	JP 8-242224 A (女屋達廣) 1996. 09. 17, 全文 (ファミリーなし)	6, 8, 9
		1-14